Terminal de teléfono de emergencia

Manual de usuario

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Prefacio

General

Este manual presenta la instalación, las funciones y las operaciones del terminal telefónico de emergencia (en lo sucesivo, "el dispositivo"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Modelos

DHI-VTA8311AB-4, DHI-VTA8311AB, DHI-VTA8311A-4, DHI-VTA8311A

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
DANGER	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
NOTE	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	junio 2022

Aviso de protección de privacidad

Como usuario del dispositivo o panel de control de datos, puede recopilar datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas.

Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo y cumpla con las pautas cuando lo use.

Requisitos de transporte

- Transporte el dispositivo en condiciones de humedad y temperatura permitidas.
- Embale el dispositivo con embalaje proporcionado por su fabricante o embalaje de la misma calidad antes de transportarlo.
- No ejerza demasiada presión sobre el dispositivo, no lo vibre violentamente ni lo sumerja en líquido durante el transporte.

Requisitos de almacenamiento

- Guarde el dispositivo en condiciones de humedad y temperatura permitidas.
- No coloque el dispositivo en un lugar húmedo, polvoriento o extremadamente cálido o frío que tenga una fuerte radiación electromagnética.
- No ejerza mucha presión sobre el dispositivo, no lo vibre violentamente ni lo sumerja en líquido durante el almacenamiento.

Requisitos de operación

- Asegúrese de que la fuente de alimentación sea correcta antes de su uso.
- No desconecte el cable de alimentación del lateral del dispositivo mientras el adaptador está encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, use y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo.

requerimientos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al dispositivo.

- El personal que trabaje en alturas debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.

- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con protección a tierra.
- Temperatura de funcionamiento: –30 °C a +65 °C (–22 °F a +149 °F).
- Al instalar el dispositivo, asegúrese de que el enchufe de alimentación y el acoplador del dispositivo puedan alcanzarse fácilmente para cortar la alimentación.
- Evite que el líquido gotee o salpique sobre el dispositivo. No coloque ningún objeto lleno de líquido, como un jarrón, encima del dispositivo.

Requisitos de mantenimiento

WARNING

Apague el dispositivo antes del mantenimiento.

Tabla de contenido

1. Información general

1.1 Introducción

Especialmente diseñado para emergencias, la terminal telefónica de emergencia de la serie VTA8 es un dispositivo de emergencia que se comunica con el centro de recepción de alarmas con solo presionar un botón. Tiene una cámara HD de 2 MP, micrófono de alta sensibilidad, dos puertos de red y un módulo 4G opcional integrado en su diseño. Altamente intuitivo, presenta funciones como audio bidireccional y transmisión de voz, y para modelos seleccionados, el dispositivo puede abrir sus propios compartimentos de forma remota.

Conveniente y fácil de usar, el dispositivo tiene un módulo PSTN incorporado que se conecta a la línea telefónica y se vincula con el centro de recepción de alarmas, lo que le permite realizar llamadas directamente desde el dispositivo. También es compatible con domos de velocidad externos, cámaras tipo bala y pantallas LED, y se puede usar en escuelas, plazas públicas, estaciones de tránsito, áreas escénicas, hospitales y más.

1.2 Funciones

El dispositivo se puede conectar a la plataforma ICC y configurar en la página web.

- Admite alarma de una sola pulsación.
- La plataforma puede hacer videos, tomar instantáneas y monitorear la terminal de alarma.
- La plataforma puede transmitir a múltiples terminales de alarma simultáneamente.
- Tarjeta electrónica.
- Amplíe con IPC, domo de velocidad y cámara instantánea.
- La pantalla de matriz de puntos se puede conectar para mostrar información.
- La pantalla LCD incorporada de 10 pulgadas puede reproducir anuncios y proporcionar información de orientación (solo aplicable en modelos seleccionados).
- Desbloqueo remoto (solo aplicable en modelos seleccionados).

2 Desembale y compruebe

Cuando reciba el dispositivo, verifique los artículos en su paquete con la siguiente lista de verificación. Si alguno de los artículos falta o está dañado, comuníquese con el minorista local o el servicio posventa de inmediato.

Tabla 2-1 Desembalar y comprobar

No.	Artículo		Contenido
1	Paquete completo	Apariencia	Sin daños evidentes.
		Paquete	Si hay signos de impactos accidentales.
		Accesorio	Si los accesorios están completos.
2	Caja	Apariencia	Sin daños evidentes.
		Cables de datos, alimentación cables, cables de ventilador y placa principal	Sin conexiones sueltas. Contactar con el servicio postventa inmediatamente si alguno de los cables o las líneas están sueltas.
3	Guía de inicio rápido		—

3 Estructura

3.1 Puertos de la placa base

Figura 3-1 Puertos de la placa base

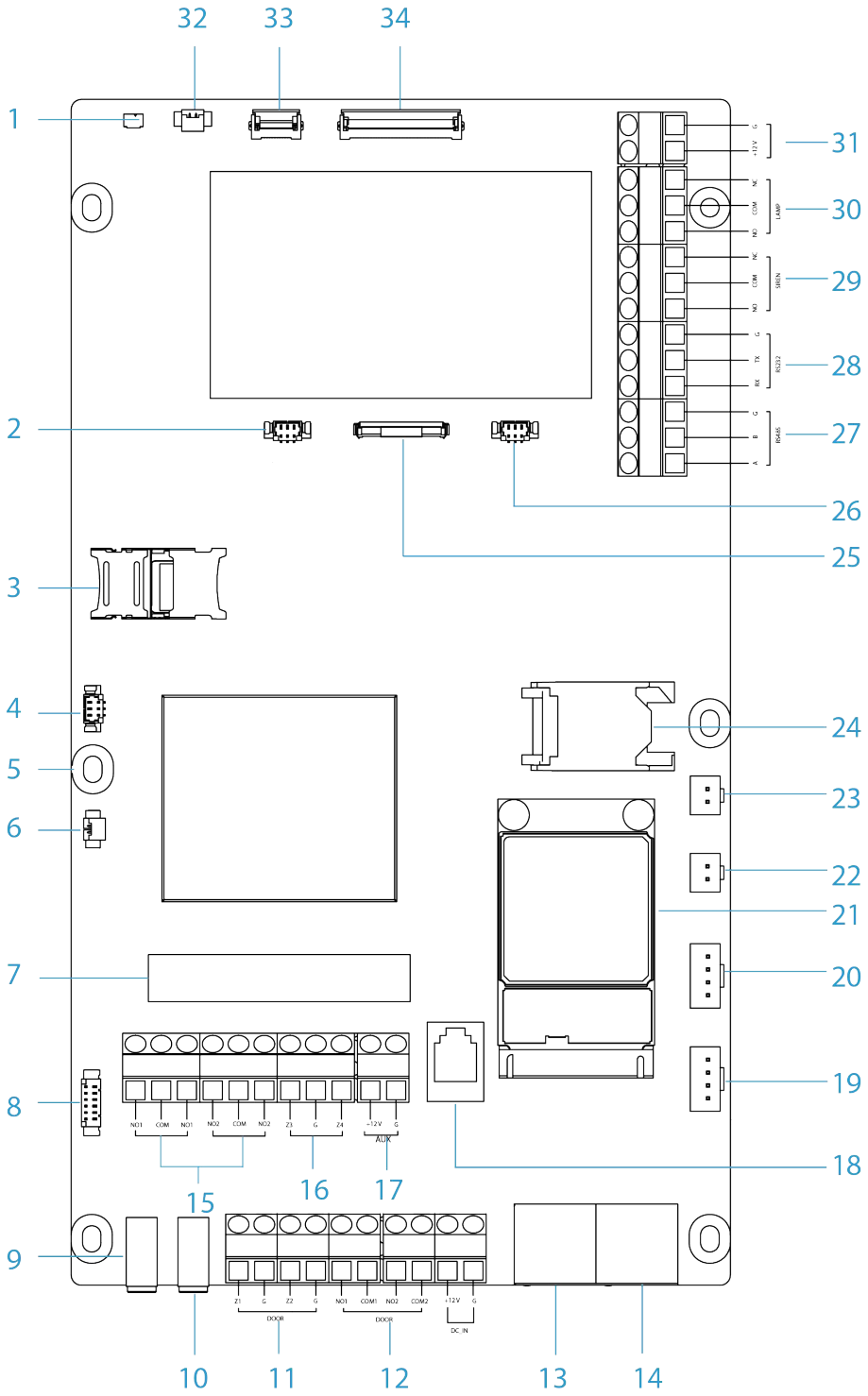


Tabla 3-1 Puertos de la placa base

No.	Nombre	No.	Nombre	No.	Nombre
1	Puerto de temperatura LCD	13	NIC2	25	Puerto de sensores
2	Módulo iluminador	14	NIC1	26	Módulo iluminador
3	ranura para tarjetas SD	15	Salida de alarma	27	RS-485
4	Módulo calentador LCD	dieciséis	Entrada de alarma	28	RS-232
5	Control del calentador módulo	17	Fuente auxiliar Puerto de salida	29	puerto sirena
6	Puerto de micrófono	18	toma de teléfono	30	Puerto de luz de alarma
7	módulo RTPC	19	Botón de alarma 2	31	Luz de alarma/sirena Puerto de alimentación
8	Puerto para deslizar tarjetas	20	Botón de alarma 1	32	Módulo LCD
9	Salida de los altavoces	21	módulo 4G	33	Puerto de pantalla táctil
10	Puerto de entrada de micrófono	22	Altavoz 1	34	puerto de pantalla LCD
11	Puerto de manipulación	23	Altavoz 2	—	—
12	Puerto de control de bloqueo	24	Ranura para tarjeta SIM	—	—

El botón de alarma 2 no está disponible actualmente.

3.2 Panel frontal

Figura 3-2 Panel frontal

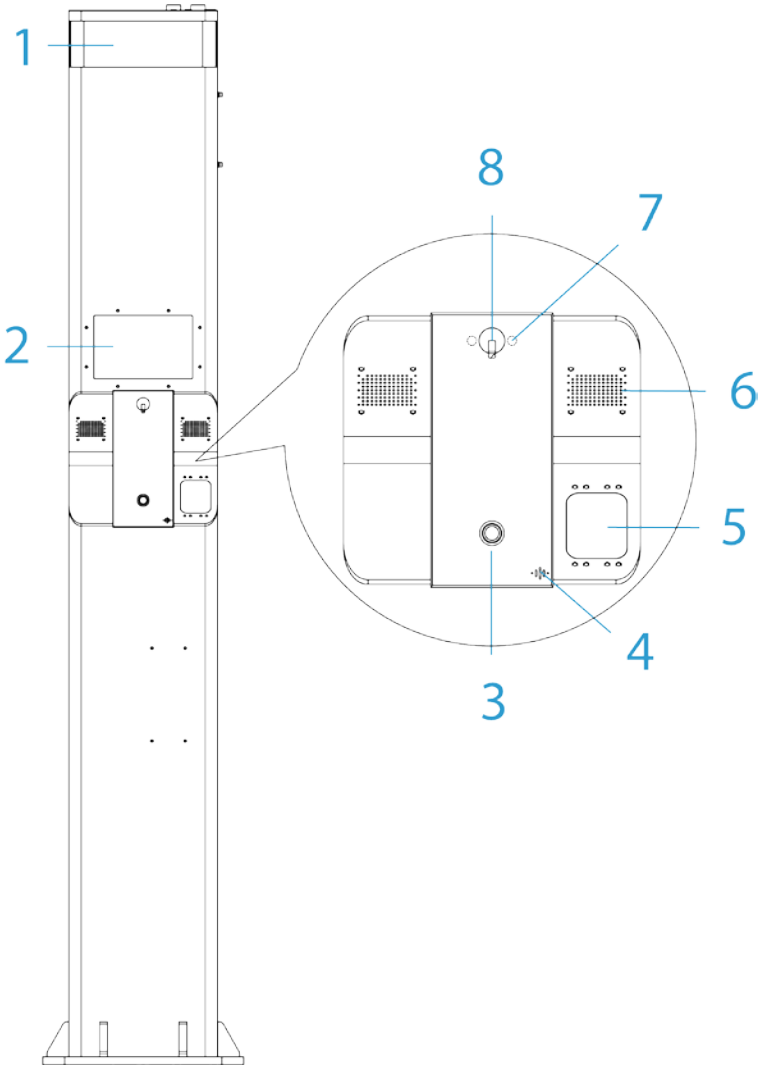


Tabla 3-2 Descripción del panel frontal

No.	Nombre	Descripción
1	Luz de alarma	Indica que se disparó una alarma. ● Normal: Sólido encendido. ● Siendo llamado: Primero parpadea y luego vuelve al estado normal.
2	pantalla LCD	Reproduce imágenes o videos y muestra el estado de la llamada.
3	Botón de alarma	Pulsa el botón para llamar al centro de gestión o a la plataforma ICC en caso de emergencia.
4	Micrófono	Entrada de audio.
5	Área de deslizamiento de tarjetas	Soporta reconocimiento de tarjeta IC.
6	Vocero	Salida de audio.
7	Iluminador	Proporciona luz IR para entornos oscuros.
8	Cámara	Captura imágenes visuales frente a la terminal de alarma.

3.3 Panel trasero

Hay 2 tipos del dispositivo.

- Tipo básico: Diseñado con cerradura mecánica.
- Tipo electrónico: Diseñado con llave electrónica.

Figura 3-3 Panel trasero (básico)

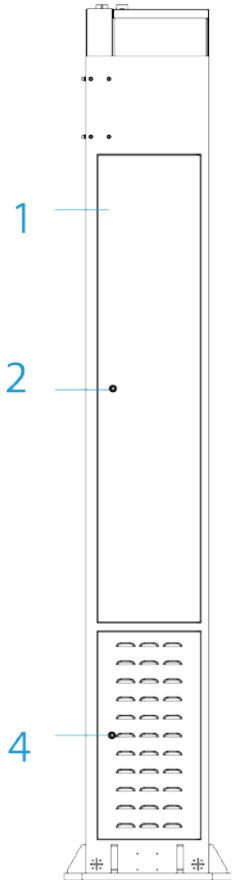


Figura 3-4 Panel trasero (electrónico)

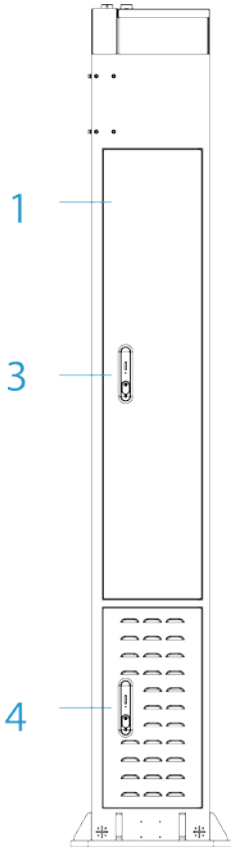
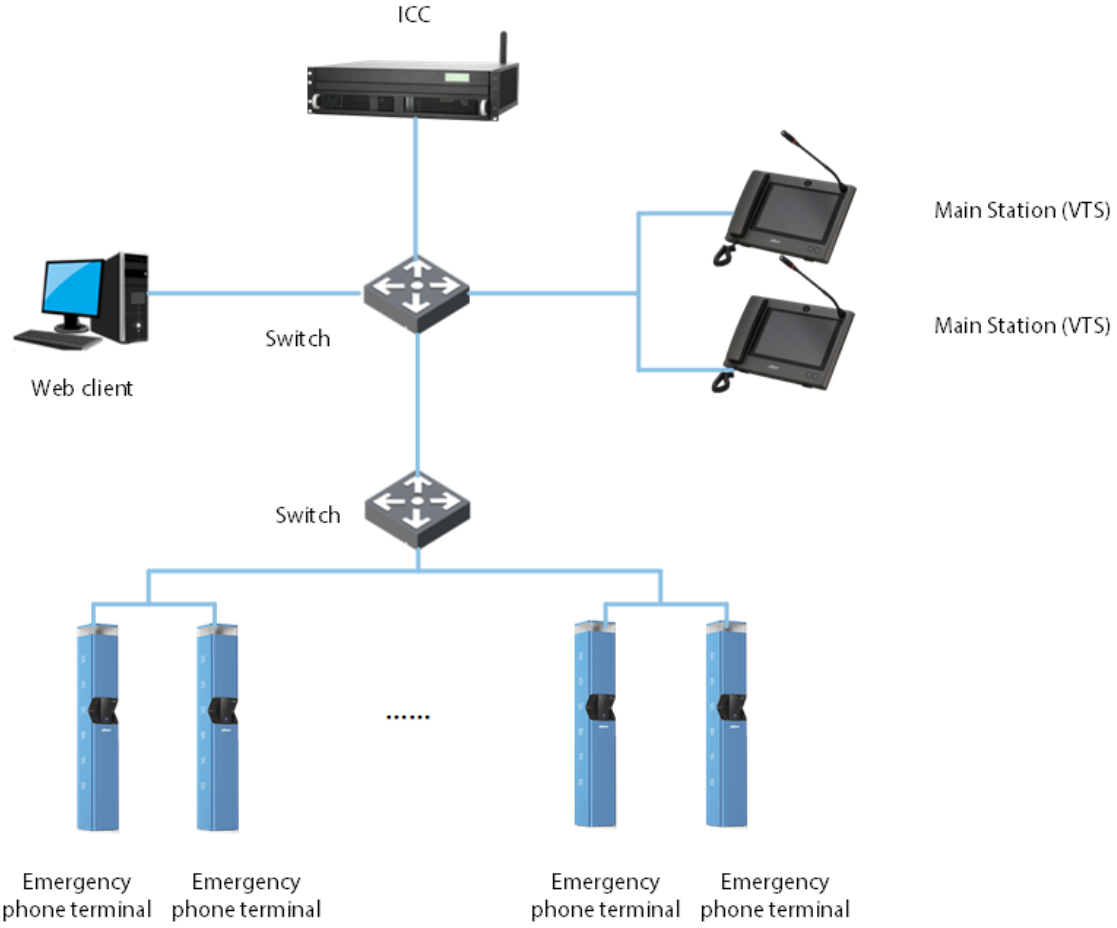


Tabla 3-3 Descripción del panel trasero

No.	Nombre	Descripción
1	Mantenimiento compartimiento	Abra el compartimiento de mantenimiento para realizar el mantenimiento del dispositivo interno.
2	cerradura mecanica	Desbloqueo con llave.
3	llave electronica	Desbloqueo remoto a través de la plataforma o administrador web del dispositivo.
4	Compartimento de herramientas	Almacena herramientas.

4 Redes

Figura 4-1 Diagrama de red



5 Instalación y cableado

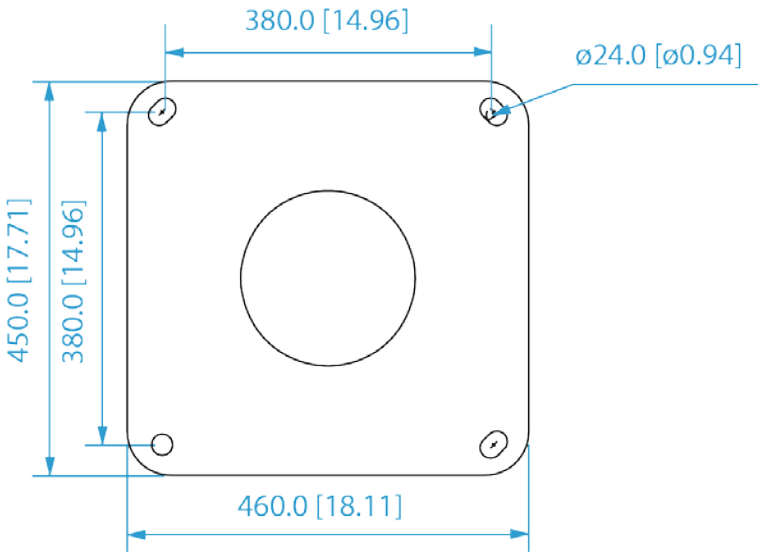
- No instale el dispositivo en un ambiente pobre que tenga condensación, altas temperaturas, manchas, polvo y está expuesto a productos químicos corrosivos.
- La instalación y la depuración deben ser realizadas por un equipo profesional. No desmonte ni reparar el dispositivo sin asistencia profesional para evitar dañar el dispositivo.

5.1 Dimensiones

Antes de la instalación, asegúrese de conocer las dimensiones del pedestal y el espacio entre el agujeros de tornillo.

Cada orificio para tornillo tiene 24 mm de diámetro, por lo que la barra de acero reforzado que atraviesa el orificio debe tener 20 mm. mm de diámetro.

Figura 5-1 Dimensiones (Unidad: mm [pulgadas])



5.2 Instalación

5.2.1 Construyendo los cimientos

Le recomendamos que siga los estándares de la industria al instalar el dispositivo, como excavar zanjas, enterrar tuberías, tender cables y realizar pruebas de aislamiento.

Paso 1 Seleccione la ubicación de instalación del dispositivo de acuerdo con los planos de construcción.

Mientras hace su selección, le recomendamos considerar condiciones tales como cableado, drenaje y ventilación.

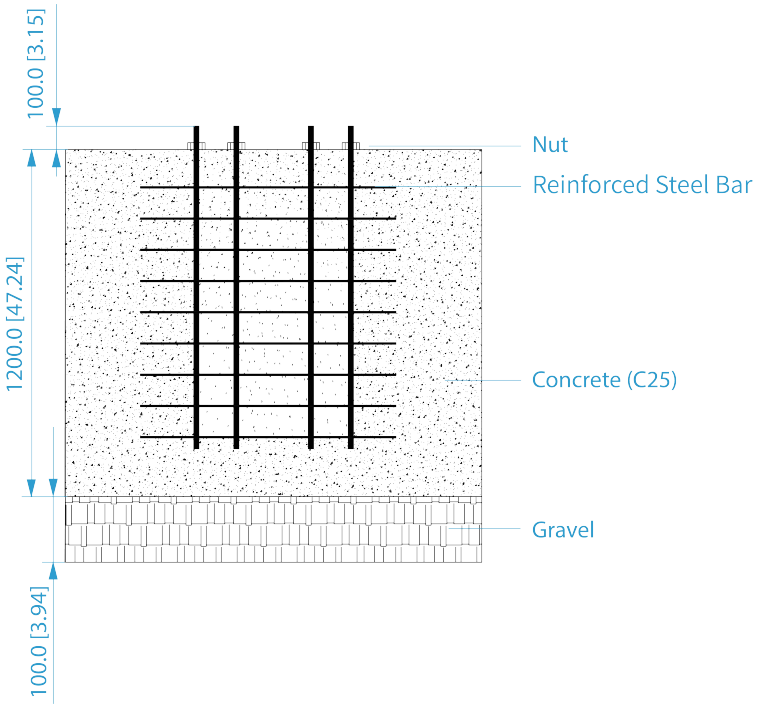
Paso 2 Cava un surco.

Paso 3 Incrustar tuberías.

Etapa 4 Construye los cimientos.

1) En la parte inferior de los cimientos, pavimentar gravas de unos 100 mm de altura.

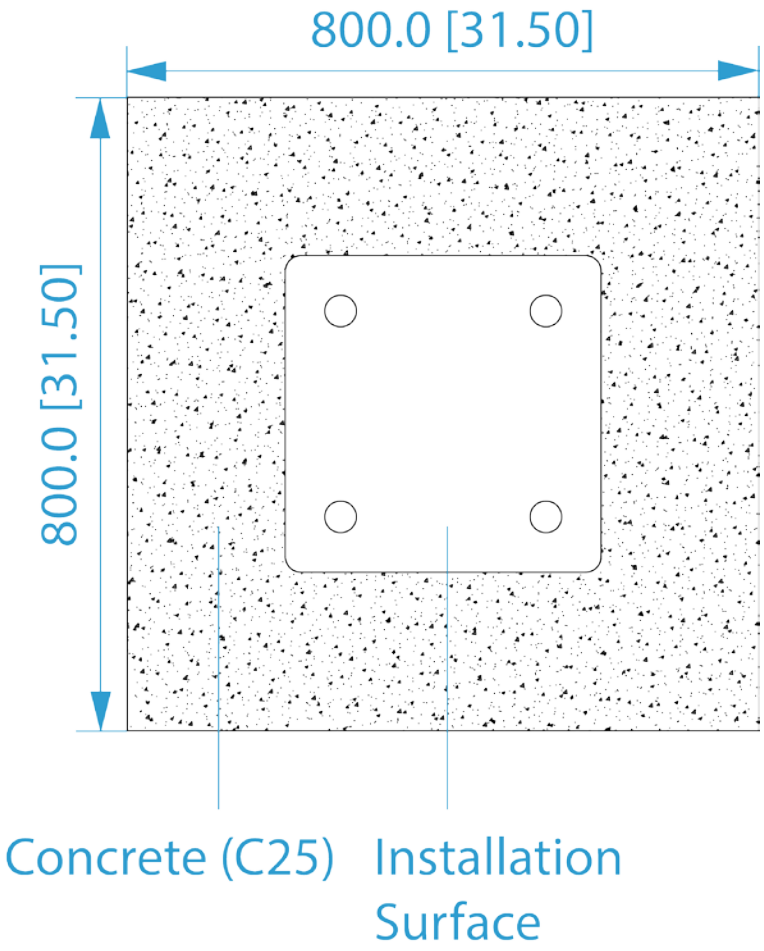
Figura 5-2 Construir los cimientos



2) Rellénelo con cemento C25. El largo y la altura no deben ser inferiores a 800 mm, y el ancho no debe ser inferior a 1200 mm.

La longitud, el ancho y la profundidad de la cimentación deben ajustarse según el textura del suelo, y la experiencia de los profesionales con las construcciones. El la medida de 800 mm y 1200 mm es solo para su referencia.

Figura 5-3 Tamaño de la base (Unidad: mm [pulgadas])



3) En hormigón C25, inserte cuatro barras de acero reforzado de 20 mm según el espacio entre los orificios para tornillos.

4) Tienda los cables.

5) Realice la prueba de aislamiento.

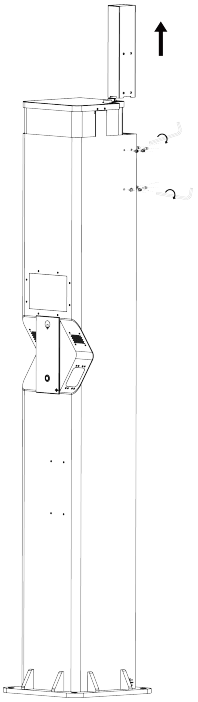
6) Instale el dispositivo.

Guíe las barras de acero reforzado de 20 mm a través de los 4 orificios del pedestal y luego apriételas y fíjelas con los tornillos M20.

5.2.2 Montaje en poste

Paso 1 Retire los tornillos con un destornillador para sacar el poste en forma de cilindro.

Figura 5-4 Saque el poste en forma de cilindro



Paso 2 Coloque el poste en forma de L y luego asegure el dispositivo con el tornillo.

Figura 5-5 Coloque el poste en forma de L

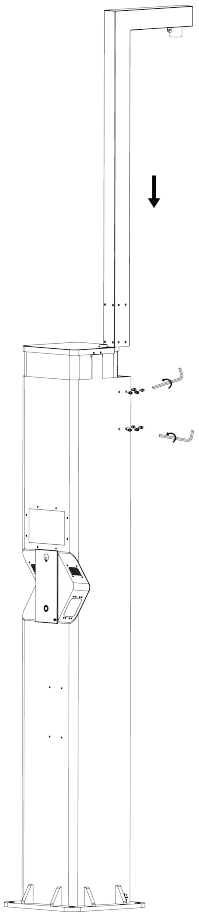
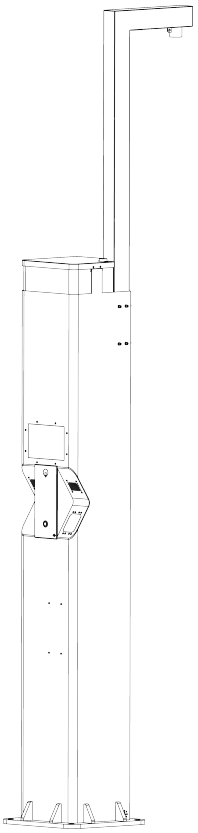


Figura 5-6 Montaje en poste



5.3 Cableado

Los módulos internos se conectaron al dispositivo antes de que saliera de fábrica

Para el tipo básico del dispositivo, solo necesita conectar corriente alterna externa y una red externa. Esta sección utiliza el cableado del tipo básico como ejemplo.

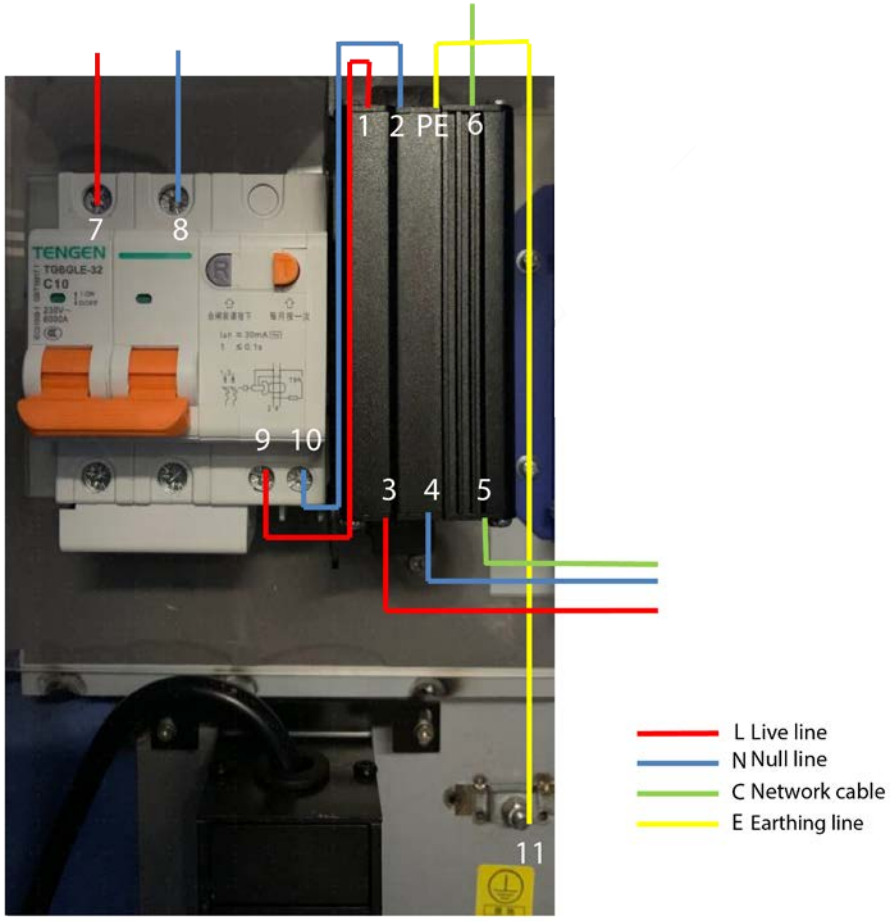
5.3.1 Conexión del puerto de alimentación de CA externo

WARNING

Antes de conectar el dispositivo, asegúrese de que el disyuntor de aire esté apagado. Después de que termines cableado del dispositivo, encienda el disyuntor de aire y el dispositivo se encenderá.

Conecte la red eléctrica a los números 7 y 8. La línea de tierra número 11 debe estar conectada a PE.

Figura 5-7 Conexión de corriente alterna externa



5.3.2 Conexión de red

Figura 5-8 Conexión de red

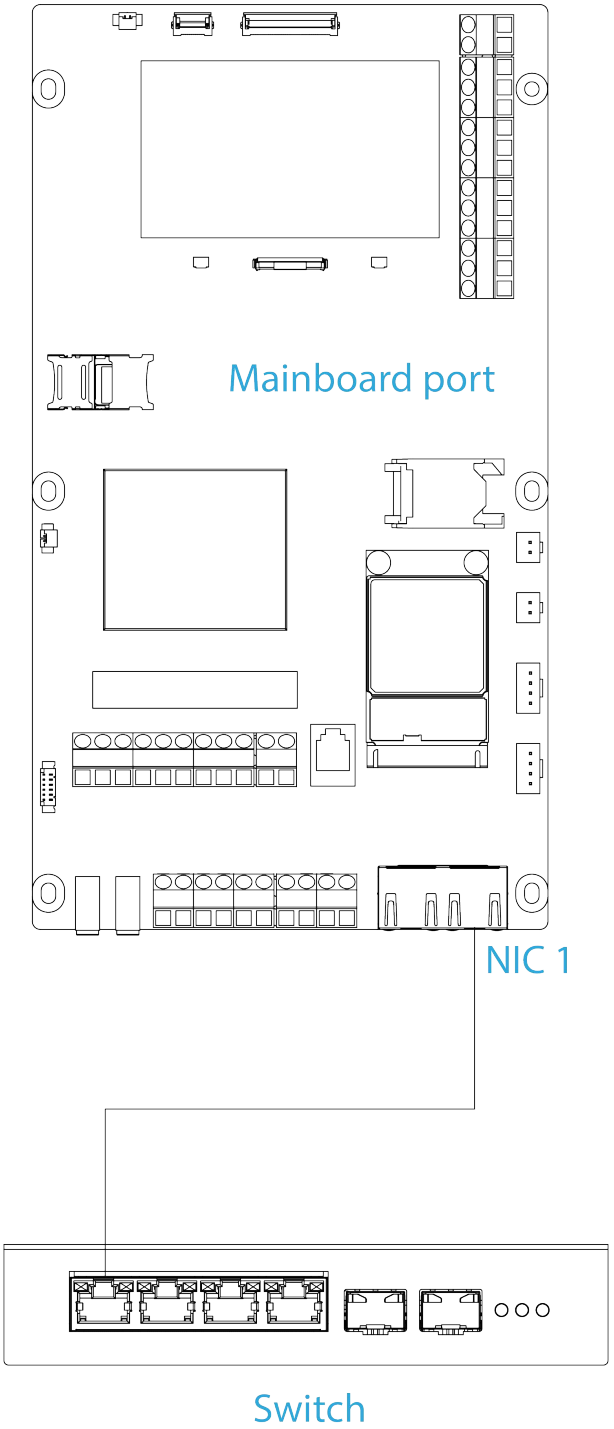


Figura 5-9 Puerto de entrada de red

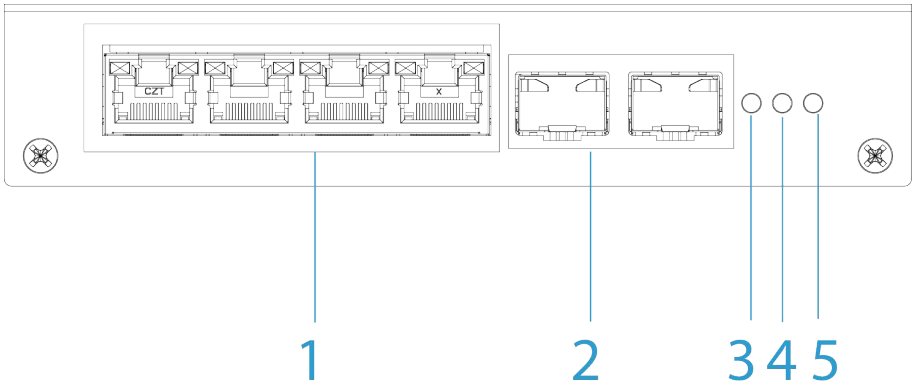


Tabla 5-1 Descripción del puerto de entrada de red

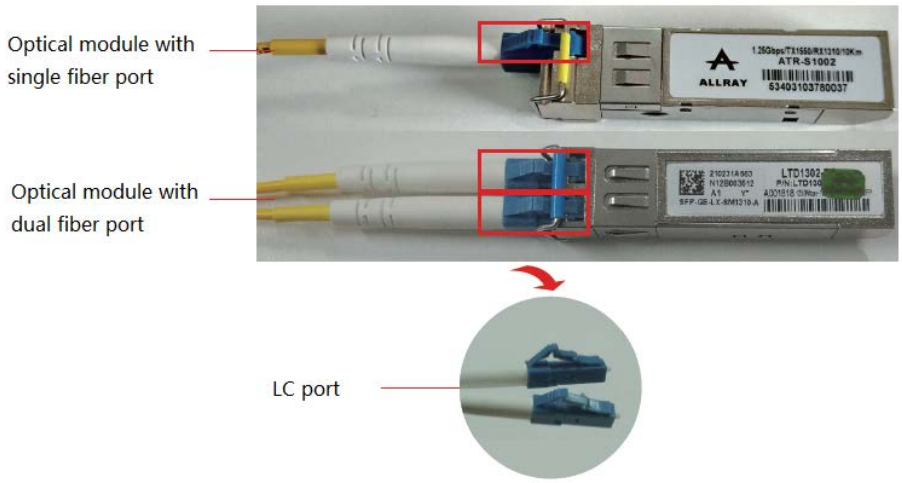
No.	Nombre	Descripción
1	10/100/1000 Base-T	Hay cuatro puertos eléctricos autoadaptativos de 10/100/1000 Mbps.
2	1000 Base-X	Hay dos puertos ópticos de 1000 Mbps.
3	Indicador de fibra óptica	—
4		
5	Indicador de encendido	

El dispositivo admite conexión de fibra.

- Conexión por cable: A través del puerto Ethernet RJ–45 (número 5) en la Figura 5-7, conecte la red externa. Luego pase un cable de red desde el puerto Ethernet RJ–45 (número 6) en la Figura 5-7 al puerto gigabit (número 1) en la Figura 5-9.
- Conexión de fibra: si se instala una fibra óptica, conecte la red externa al puerto de fibra óptica de la Figura 5-10.

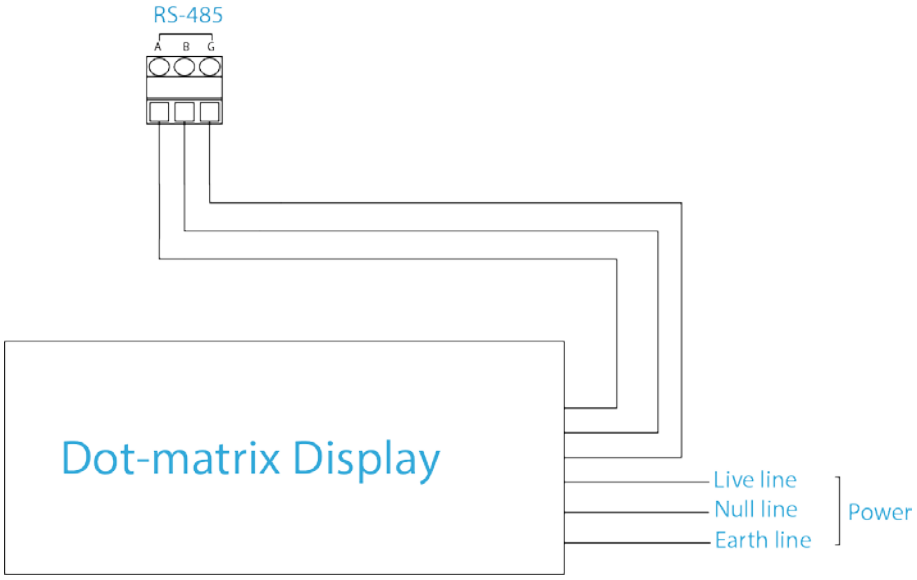
La recepción y el envío de las bandas de ondas de trabajo y el ancho de banda de los módulos ópticos en ambos Los extremos de la fibra óptica deben coincidir. De lo contrario, la red no funcionará correctamente.

Figura 5-10 Puerto de módulo óptico de fibra simple o doble



5.3.3 Conexión de pantalla de matriz de puntos

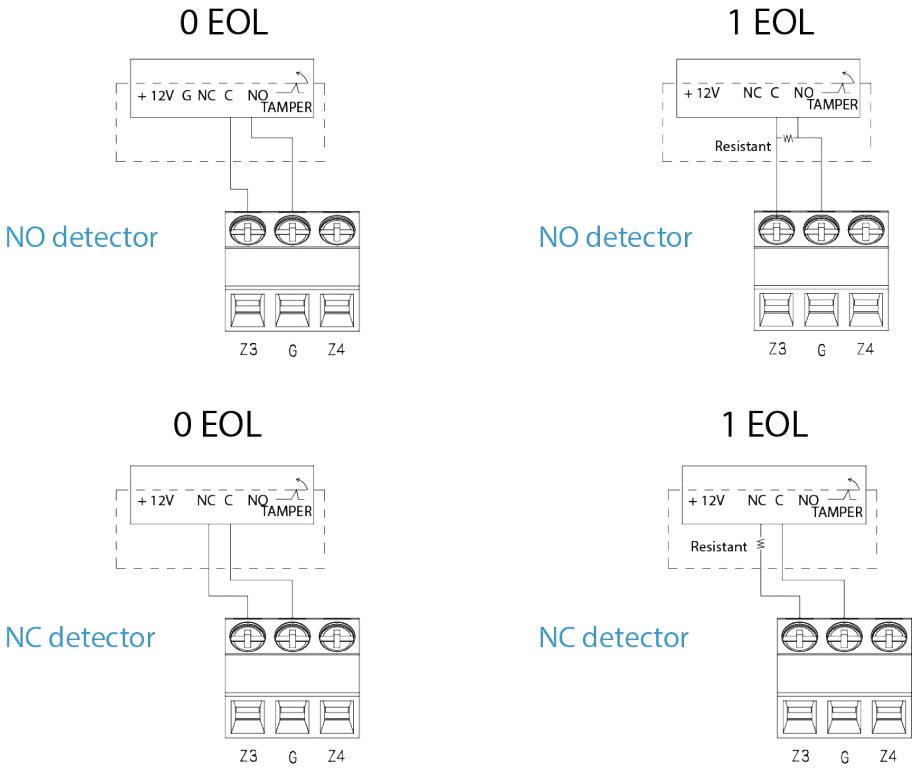
Figura 5-11 Conectar pantalla de matriz de puntos



5.3.4 Conexión del cable de entrada de alarma local

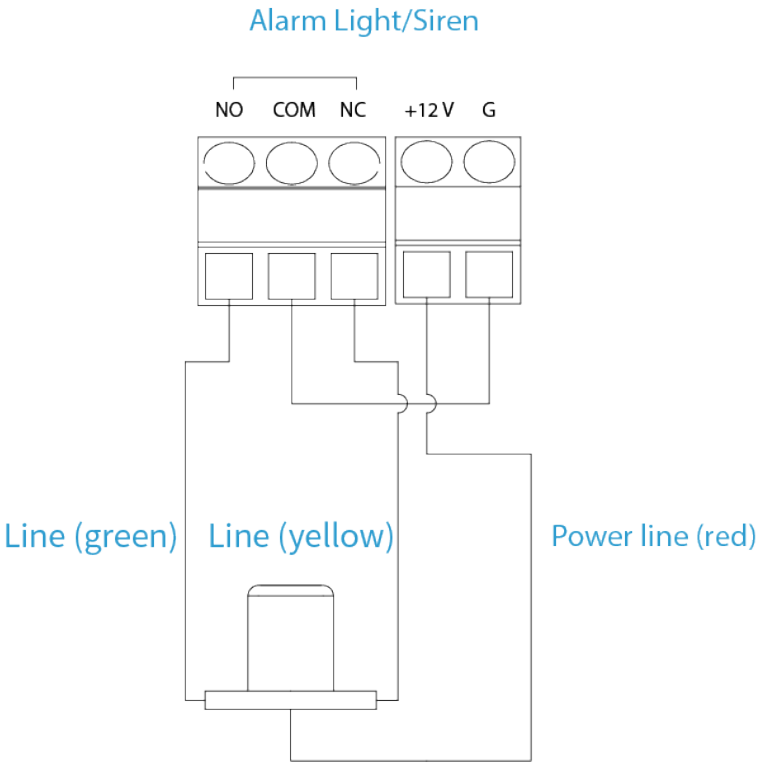
El dispositivo admite 0 EOL y 1 EOL.

Figura 5-12 Cableado del detector



5.3.5 Conexión del cable de salida de alarma local

Figura 5-13 Conexión del cable de salida de alarma local



- Línea eléctrica: Positiva (pública).
- Línea (amarilla): Negativo. Cuando la línea amarilla está conectada, la luz de alarma permanecerá encendida.
- Línea (verde): Negativo. Cuando la línea verde está conectada, la luz de alarma parpadeará.

6 Operaciones web

Esta sección presenta los parámetros del dispositivo y cómo configurarlos en la página web.

Algunas operaciones del dispositivo están disponibles en la plataforma. Para las operaciones de la plataforma, consulte el correspondiente manual de usuario de la plataforma.

6.1 Iniciar el dispositivo

6.1.1 Inicialización del dispositivo

Información de contexto

Para el uso por primera vez después de restaurar el dispositivo a los valores predeterminados de fábrica, debe configurar la contraseña de inicio de sesión para la cuenta de administrador. También puede reservar una dirección de correo electrónico para restablecer la contraseña cuando la olvide.

- Para la seguridad de su dispositivo, mantenga su contraseña de inicio de sesión de administrador mucho después de la inicialización, y cambiar la contraseña regularmente.
- La dirección IP predeterminada de LAN1 es 192.168.1.108, LAN2 es 192.168.2.108.

Procedimiento

Paso 1 Abra el navegador, ingrese la dirección IP predeterminada del dispositivo y luego presione la tecla Enter. Leer

Paso 2 **acuerdo de licencia de software**y**política de privacidad**, seleccionar**He leído y acepto los términos del Acuerdo de licencia de software y la Política de privacidad**y luego haga clic en**Próximo**. Seleccione el idioma y

Paso 3 luego haga clic en**Próximo**.

Etapa 4 Establezca el formato de fecha, la zona horaria y la hora del sistema y luego haga clic en**Próximo**.

Hacer clic**Sincronizar PC**para sincronizar la hora del sistema con la PC.

Paso 5 Ingrese y confirme la nueva contraseña, configure la dirección de correo electrónico y luego haga clic en**Próximo**.

La dirección de correo electrónico reservada se utiliza para recibir el código de seguridad para restablecer la contraseña.

Paso 6 Hacer clic**Terminado**.

El sistema le indicará que la inicialización fue exitosa y luego se mostrará la página de inicio de sesión.

6.1.2 Iniciar sesión en la página web

Requisito previo

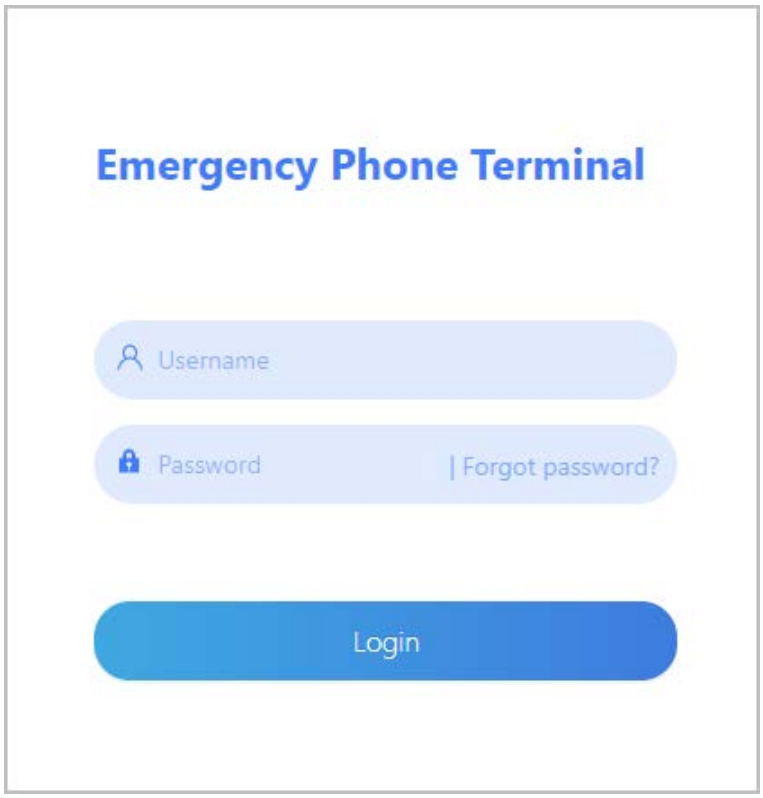
Asegúrese de que la computadora local y el dispositivo estén en el mismo segmento de red.

Procedimiento

Paso 1 Ingrese la dirección IP del dispositivo en la barra de direcciones del navegador y luego presione Enter. Ingrese

Paso 2 el nombre de usuario y la contraseña, y luego haga clic en**Acceso**.

Figura 6-1 Inicio de sesión



6.1.3 Restablecimiento de contraseña

requisitos previos

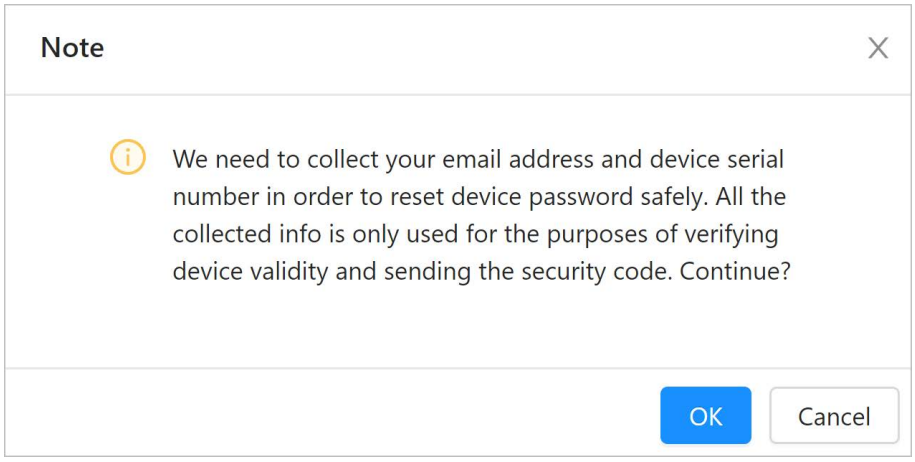
Puede configurar la dirección de correo electrónico para restablecer la contraseña durante la inicialización. Para obtener más información, consulte "6.1.1 Inicialización del dispositivo".

Procedimiento

Paso 1 Inicie sesión en la página web, haga clic en**¿Has olvidado tu contraseña?**. Hacer clic**DE**

Paso 2 **ACUERDO**.

Figura 6-2 Contraseña olvidada



Paso 3 Escanee el código QR de acuerdo con la indicación para recibir el código de seguridad. Introduzca el código

Etapa 4 de seguridad en el**Código de seguridad**cuadro de texto y, a continuación, haga clic en**Próximo**.

Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, se convertirá inválido.

Paso 5 Ingrese y confirme la contraseña.

La contraseña puede contener de 8 a 32 caracteres no vacíos y debe tener al menos 2 tipos de los siguientes caracteres: letras mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; , : &). La contraseña de confirmación debe ser la misma que la nueva contraseña Utilice el indicador de seguridad de la contraseña como guía para establecer una contraseña segura.

Paso 6 Hacer clic**Finalizar**.

6.2 Generalidades

Sobre el**General**página, puede configurar los ajustes generales, como enlace de llamadas, PSTN, zonas, videos, audios y desbloqueo de compartimentos.

6.2.1 Vinculación de llamadas

Seleccionar**General**>**Vinculación de llamadas**, y luego puede establecer acciones de vinculación de llamadas, como instantáneas, recodificación y sirena.

Figura 6-3 Vinculación de llamadas

Tabla 6-1 Descripciones de los parámetros de vinculación de llamadas

Parámetro	Descripción
Instantánea	Habilitado por defecto. ● El intervalo de instantáneas varía de 1 a 10 segundos. 5 segundos está configurado de forma predeterminada. ● El número de imágenes oscila entre 1 y 5. El valor predeterminado es 5.
Registro	Habilitado por defecto.
Sirena	Habilitado por defecto. La duración de la sirena oscila entre 1 y 60 segundos. 30 segundos está configurado de forma predeterminada.

6.2.2 RTPC

Seleccionar**General**>**RTPC**, y luego puede configurar el número de teléfono y el umbral TSD, mediante el cual puede hacer que una voz hable con el centro de recepción de alarmas o la persona que llama.

Figura 6-4 RTPC

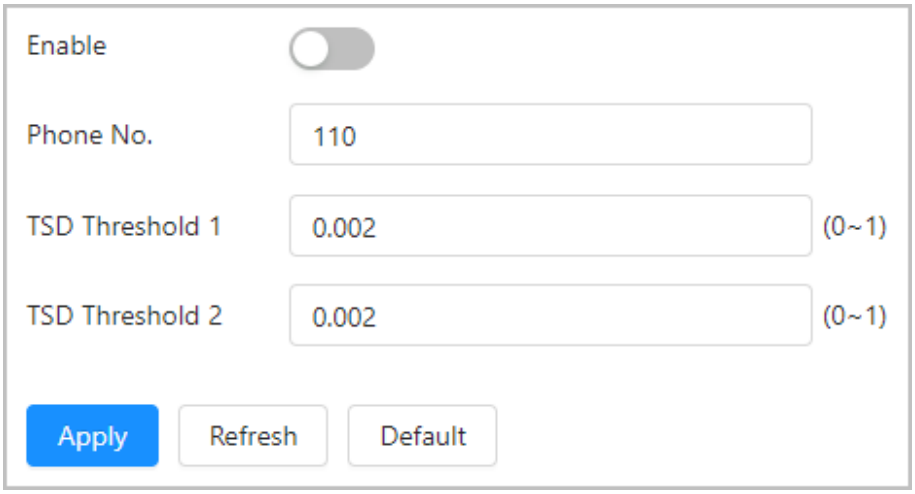


Tabla 6-2 Descripciones de los parámetros de PSTN

Parámetro	Descripción
Permitir	Deshabilitado por defecto.
Telefono no.	Ingrese el centro de recepción de alarmas o el número de teléfono personal.
TSD umbral 1	Es 0,002 por defecto, y el valor oscila entre 0 y 10. Configure los parámetros según la situación real.
TSD umbral 2	

6.2.3 Zona

6.2.3.1 Configuración de zona

Seleccionar**General**>**Zona**>**Configuración de zona**, y luego puede configurar los parámetros de zona y establecer acciones de enlace de alarma, como altavoz, relé y sirena.

Se pueden configurar hasta cuatro zonas.

Figura 6-5 Configuración de zona

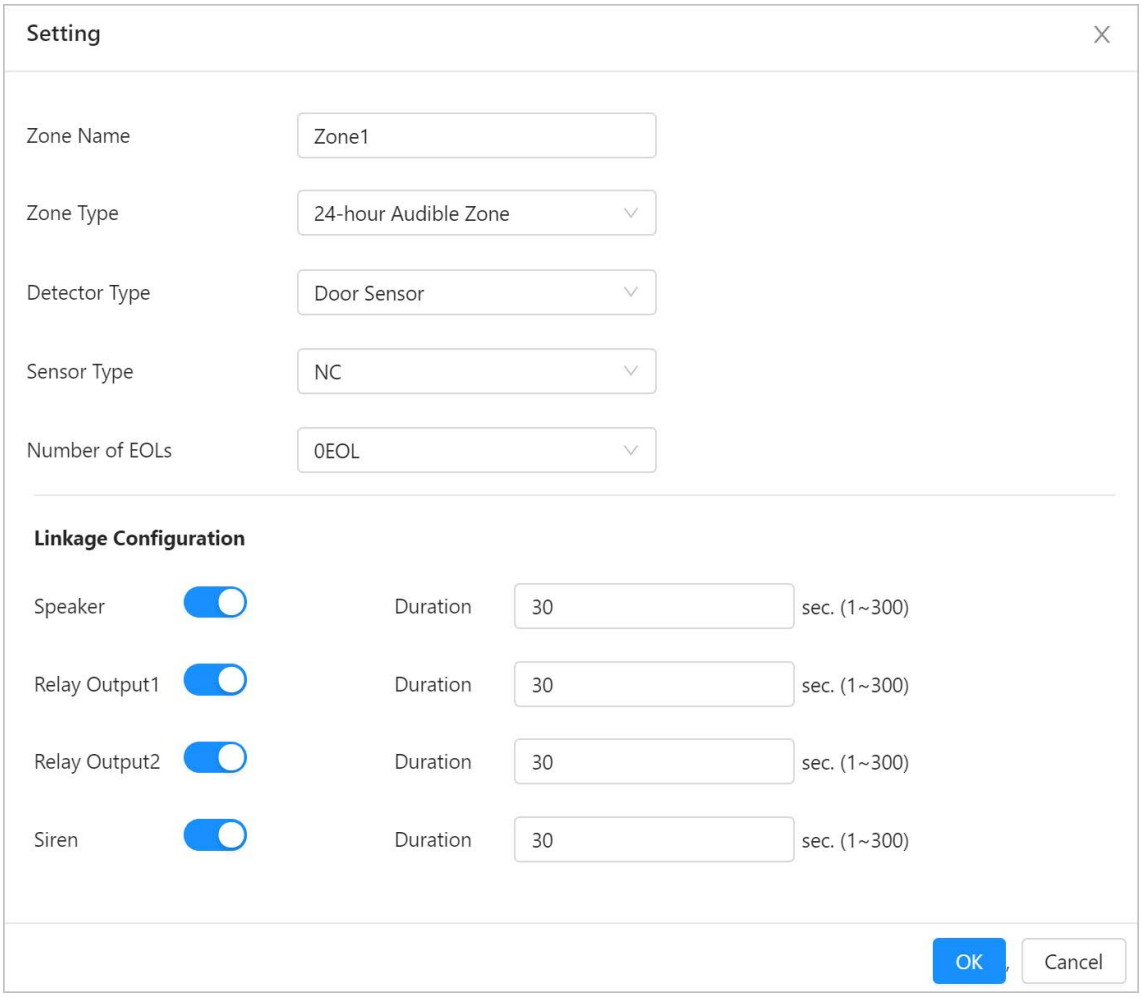


Tabla 6-3 Descripciones de los parámetros de zona

Parámetro	Descripción
Nombre de zona	Nombre de zona personalizado.
Tipo de zona	Seleccione la zona según sea necesario. ● Zona audible de 24 horas ● Zona Silenciosa 24 horas ● Zona instantánea ● Zona de fuego ● Zona blindada

Parámetro	Descripción
Tipo de detector	Seleccione el tipo de detector según sea necesario. ● Botón de pánico ● infrarrojos ● detector de puerta ● Sensor de fugas de agua ● Sensor de vibración ● Tecnología dual (IR + Microondas)
Tipo de sensor	Seleccione el tipo de sensor según sea necesario. ● Normalmente cerrado ● Normalmente abierto
Número de EOL	Seleccione el número de EOL. ● 0 EOL ● 1 EOL
Vocero	Habilitado por defecto. La duración del altavoz oscila entre 1 y 300 segundos. 30 segundos está configurado de forma predeterminada.
Salida de relé 1	Habilitado por defecto. La duración de la salida del relé varía de 1 a 300 segundos. 30 segundos está configurado de forma predeterminada.
Salida de relé 2	
Sirena	Habilitado por defecto. La duración de la sirena varía de 1 a 300 segundos. 30 segundos está configurado de forma predeterminada.

6.2.3.2 Gestión de Zonas de Protección

Seleccionar**General**>**Zona**>**Gestión de zonas de protección**, y luego puede armar y desarmar todas las zonas.

Se pueden configurar hasta cuatro zonas.

Figura 6-6 Gestión de zonas de protección

Arm Disarm

Zone No.	Zone Name	Arming Status	Zone Status
1	Zone1	Disarm	Open
2	Zone2	Disarm	Open
3	Zone3	Disarm	Normal
4	Zone4	Disarm	Normal

6.2.4 Vídeo

6.2.4.1 Codificar

Seleccionar**General**>**Video**>**Codificar**, y luego puede configurar los parámetros de la transmisión de video, como la compresión, la resolución, la velocidad de fotogramas, el tipo de velocidad de bits, la velocidad de bits, el intervalo de fotogramas I, SVC y la marca de agua.

Figura 6-7 Codificar

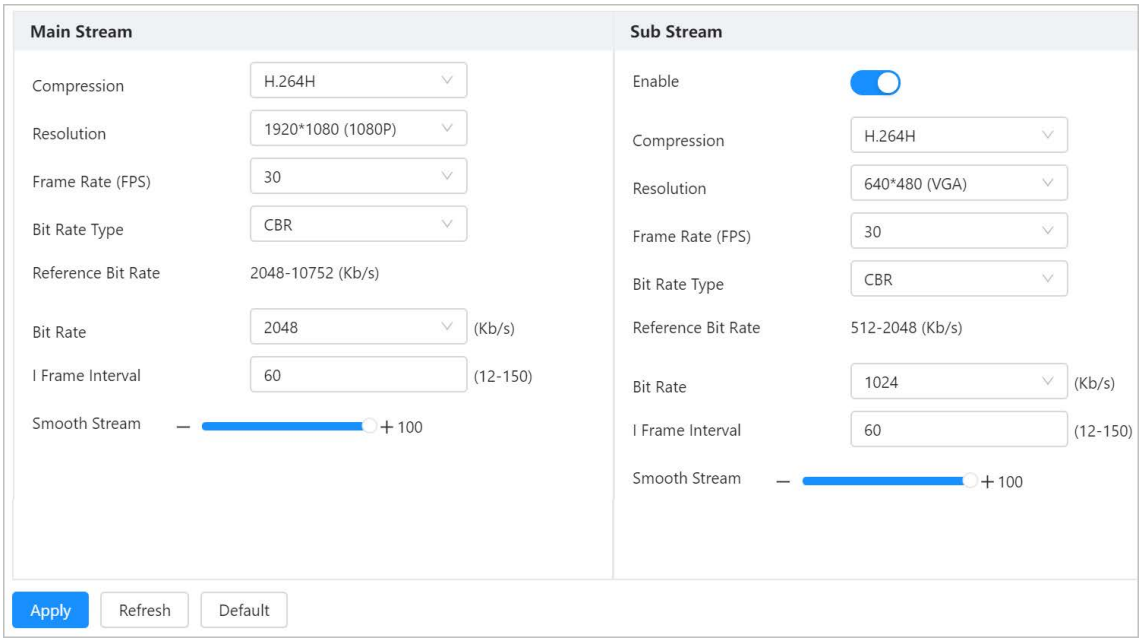


Tabla 6-4 Descripción de los parámetros de codificación

Parámetro	Descripción
Sub corriente	Hacer clic para habilitar la transmisión secundaria, está habilitada de manera predeterminada.
Compresión	Seleccione el modo de codificación. ● **H.264B**: Modo de codificación del perfil de línea de base. Requiere menor ancho de banda. ● **H.264**: modo de codificación del perfil principal. En comparación con H.264B, requiere un ancho de banda más pequeño. ● **H.264H**: modo de codificación de alto perfil. En comparación con H.264, requiere un ancho de banda más pequeño. ● **H.265**: modo de codificación del perfil principal. En comparación con H.264, requiere un ancho de banda más pequeño.
Resolución	La resolución del vídeo. Cuanto mayor sea el valor, más clara será la imagen, pero mayor será el ancho de banda requerido.
Velocidad de fotogramas (FPS)	El número de cuadros en un segundo de video. Cuanto mayor sea el valor, más claro y suave será el video.
Tipo de tasa de bits	El tipo de control de tasa de bits durante la transmisión de datos de video. Puede seleccionar el tipo de tasa de bits entre: ● **CBR**(Tasa de bits constante): La tasa de bits cambia un poco y se mantiene cerca del valor de tasa de bits definido. ● **VBR**(Velocidad de bits variable): la velocidad de bits cambia a medida que cambia la escena de monitoreo. El **Tipo de tasa de bits** solo se puede configurar como **CBR** cuando **Modo de codificación** se establece como **MJPEG**.
Tasa de bits de referencia	El rango de valores de tasa de bits más adecuado recomendado al usuario de acuerdo con la resolución definida y la tasa de cuadros.

Parámetro	Descripción
Tasa de bits	Este parámetro solo se puede configurar cuando el**Tipo de tasa de bits**se establece como**CBR**. Seleccione el valor de tasa de bits en la lista según la condición real.
Intervalo de fotogramas	El número de fotogramas P entre dos fotogramas I y el**Intervalo de fotogramas**el rango cambia como**FPS**cambios. Se recomienda establecer **Intervalo de fotogramas**el doble de grande que**FPS**.
Flujo suave	Arrastre la barra de desplazamiento o haga clic**+**o-para establecer el valor de flujo suave. Cuanto mayor sea el valor, más clara será la imagen.

6.2.4.2 Imagen

Seleccionar**General**>**Video**>**Imagen**, y luego puede configurar los parámetros de la cámara de acuerdo con la situación real, incluida la imagen, la exposición, la luz de fondo y el balance de blancos.

Figura 6-8 Configuración de imagen

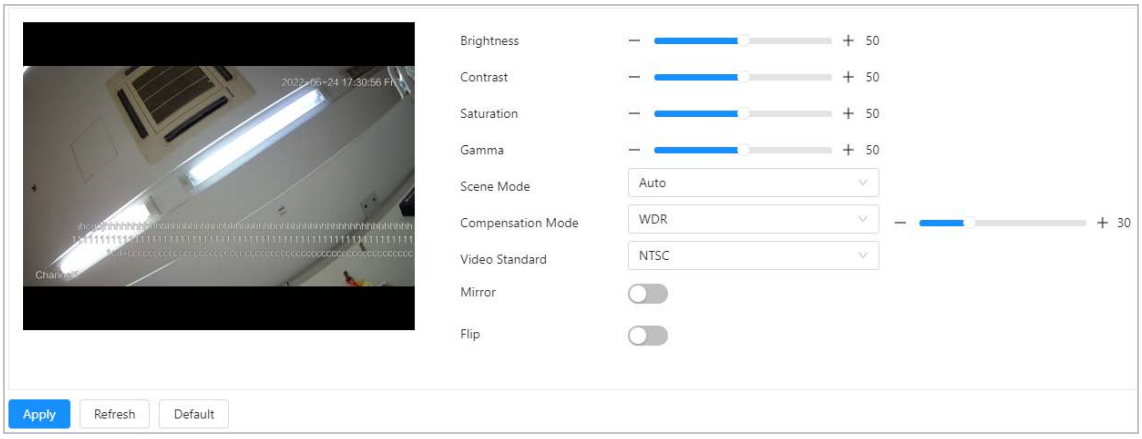


Tabla 6-5 Parámetros de configuración de imagen

Parámetros	Descripción
Brillo	Cambia el brillo general de la imagen. Cuanto mayor sea el valor, más brillante será la imagen y cuanto más pequeña, más oscura. La imagen puede verse borrosa si el valor está configurado demasiado alto.
Contraste	Cambia el contraste de la imagen. Cuanto más alto sea el valor, mayor será el contraste entre las áreas claras y oscuras, y cuanto más pequeño, menos. Si el valor es demasiado alto, el área oscura será demasiado oscura y el área brillante será más fácil de sobreexponer. La imagen puede ser gris si el valor es demasiado pequeño.
Saturación	Hace que el color sea más profundo o más claro. Cuanto más alto sea el valor, más profundo será el color y más bajo, más claro. Este valor no afecta el brillo general de la imagen.
Gama	Cambia el brillo y el contraste de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen y cuanto más pequeña, más oscura.

Parámetros	Descripción
Modo escena	● **Cerca**: Cerrar WB. ● **Auto**: El sistema compensa el balance de blancos según la temperatura del color para garantizar la precisión del color. ● **Soleado**: El sistema compensa el balance de blancos en una escena exterior soleada para garantizar la precisión del color. ● **Noche**: El sistema compensa el balance de blancos de la escena nocturna al aire libre para garantizar la precisión del color.
Modo de compensación	● **Cerca**: Sin retroiluminación. ● **CLB**: Permitir**CLB**, la cámara puede obtener una imagen más clara de las áreas oscuras del objetivo. ● **WDR**: El sistema atenúa las áreas brillantes y compensa las áreas oscuras para garantizar la claridad de toda el área de acuerdo con las condiciones de iluminación ambiental. ● **LLC**: el sistema restringe las áreas brillantes y reduce el tamaño del halo para atenuar el brillo general.
Codificación de vídeo	Seleccionar**CAMARADA**o**NTSC**.
Espejo	Hacer clic , y la imagen se mostrará con el lado izquierdo y derecho invertido
Voltear	Hacer clic , y la imagen se mostrará con los lados arriba y abajo invertido

6.2.4.3 Superposición

Seleccionar**General**>**Video**>**Cubrir**y luego configure la información de superposición, que se mostrará en la página en vivo.

6.2.4.3.1 Configuración del título del canal

Puede habilitar esta función cuando necesite mostrar el título del canal en la imagen de video.

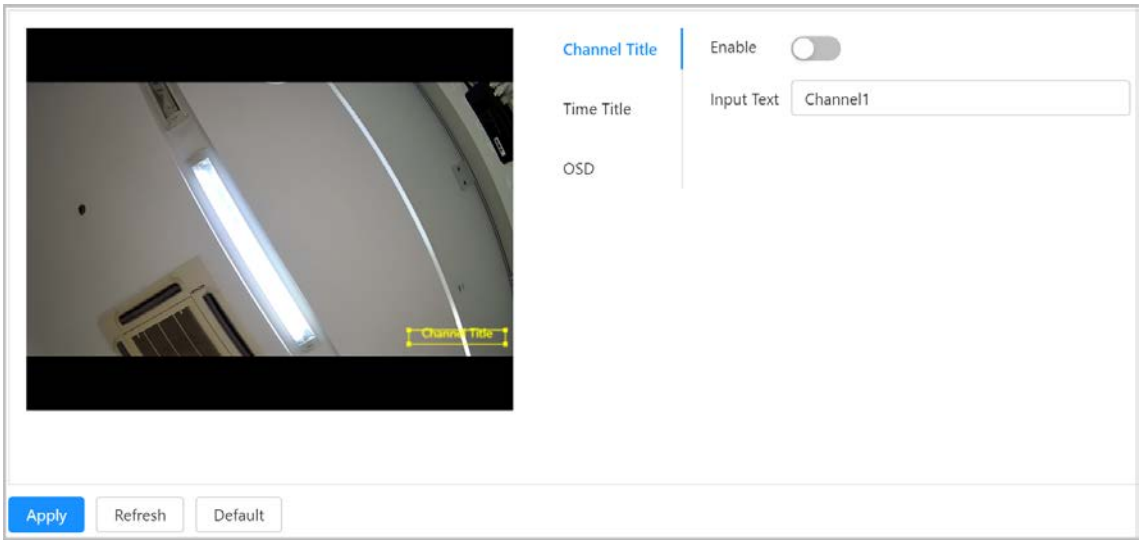
Paso 1 Seleccionar**General**>**Video**>**Cubrir**>**Título del canal**. Hacer

Paso 2 clic para habilitar la función de título de canal.

Paso 3 Configurar el título del canal.

Etapa 4 Mueva el cuadro de título a la posición que desee en la imagen.

Figura 6-9 Título del canal



Paso 5 Hacer clic**Aplicar**.

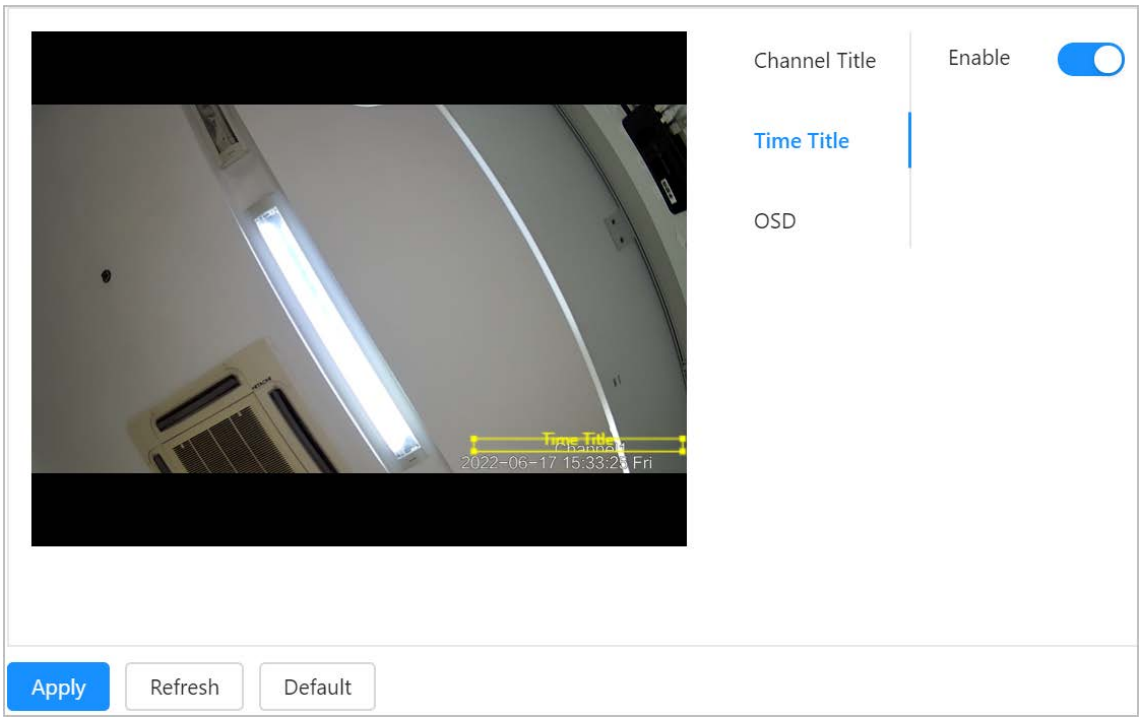
6.2.4.3.2 Configuración del título de tiempo

Puede habilitar esta función si necesita mostrar la hora en la imagen de video. Paso

1 Seleccionar**General**>**Video**>**Cubrir**>**Título de tiempo**.

Paso 2 Hacer clic para habilitar la función de título de tiempo.

Figura 6-10 Configurar título de tiempo



Paso 3 Mueva el cuadro de título a la posición que desee en la imagen. Hacer

Etapa 4 clic**Aplicar**.

6.2.4.3.3 Configuración de la información de la imagen

Configure el contenido de la información OSD y la ubicación de superposición de las imágenes capturadas.

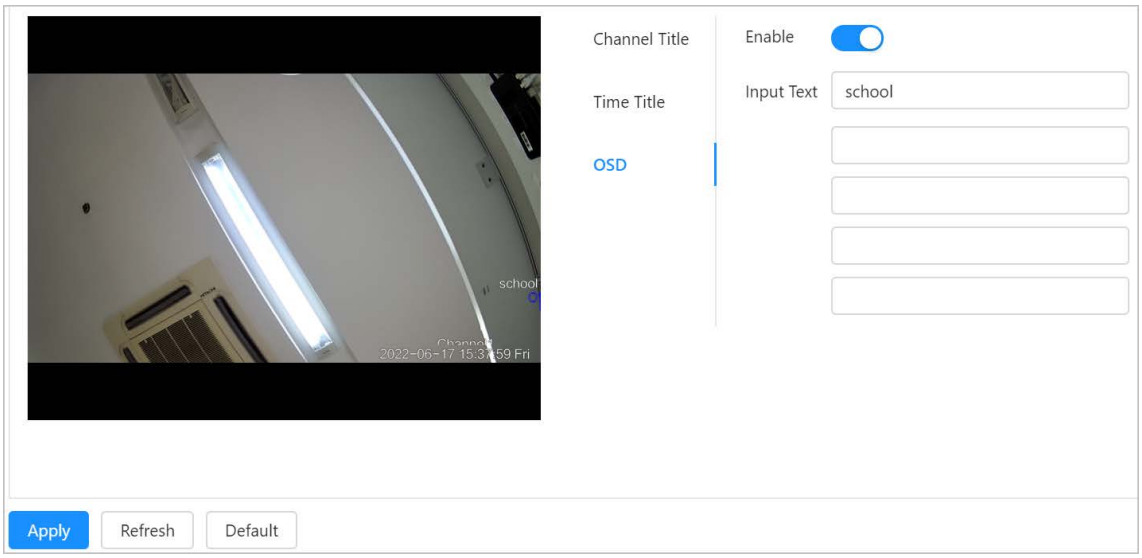
Paso 1 Seleccionar**General**>**Video**>**Cubrir**>**OSD**. Hacer

Paso 2 clic para habilitar la función OSD.

Paso 3 Introduzca el contenido OSD.

Etapa 4 Mueva el cuadro de título a la posición que desee en la imagen.

Figura 6-11 Establecer contenido OSD



Paso 5 Hacer clic**Aplicar**.

6.2.5 Audio

Seleccionar**General**>**Audio**y luego puede configurar los parámetros de audio y el audio de la alarma.

Figura 6-12 Audio

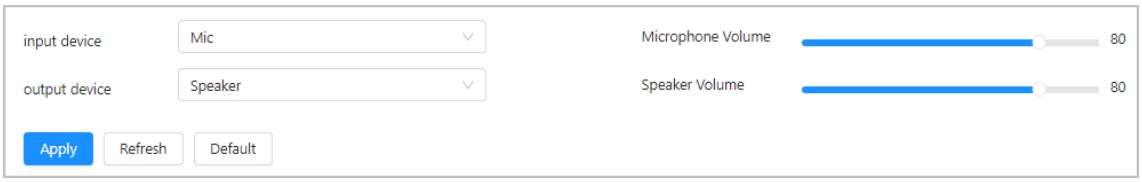


Tabla 6-6 Descripciones de parámetros de audio

Parámetros	Descripción
Dispositivo de entrada	Puede seleccionar el tipo de entrada de audio entre: ● **En línea**: Requiere un dispositivo de audio externo. ● **Micrófono**: No requiere dispositivo de audio externo.
Dispositivo de salida	Conéctese a un altavoz externo para mejorar el audio.
Volumen del micrófono	Ajusta el volumen del micrófono.
Volumen del altavoz	Ajusta el volumen del altavoz.

6.2.6 Publicidad

6.2.6.1 Configuración de recursos publicitarios

La pantalla LCD incorporada puede mostrar imágenes y videos.

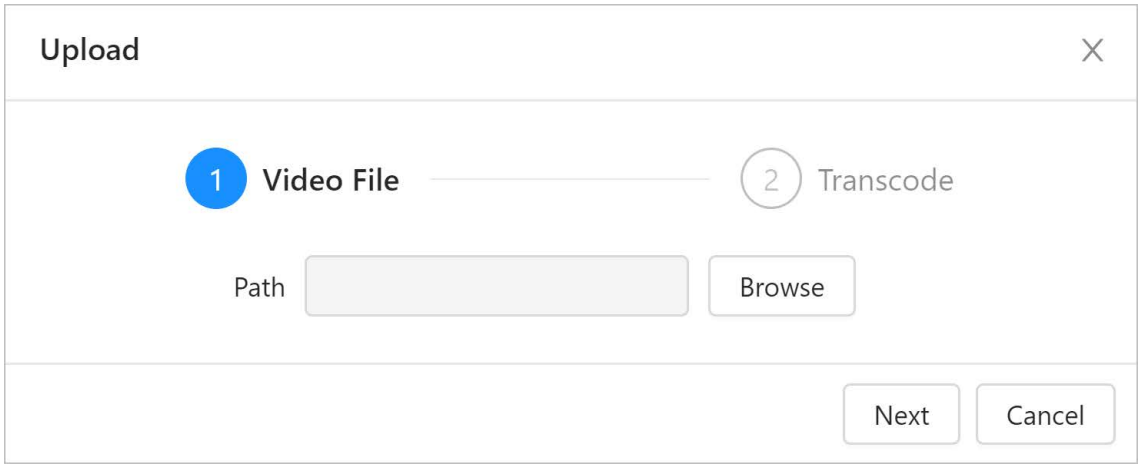
Paso 1 Seleccionar**General**>**Publicidad**>**Recurso publicitario**. Sobre el

Paso 2 **Video**área, haga clic**Subir**para subir el video. 1) Haga clic**Navegar** y luego seleccione el archivo de video.

- Puede cargar paquetes de video de hasta 20 M de tamaño, en formato avi, dav y mp4 formato.
- Puedes subir hasta 3 videos.
- Asegúrese de haber descargado el complemento para cargar el video.

2) Haga clic**Próximo**, la transcodificación está completa.

Figura 6-13 Subir archivos de video



Paso 3 Sobre el**Imagen**área, haga clic**Subir**para subir la imagen.

- Puede cargar paquetes de imágenes de hasta 2 M de tamaño, en formato png, jpg y bmp formato.
- Puedes subir hasta 10 imágenes.

Etapa 4 Establecer planes de tiempo para la publicidad.

1) En el**Plan de tiempo**área, haga clic**Agregar**para agregar el plan de tiempo de publicidad.

2) Introduzca el nombre del anuncio.

3) Configurar periodos publicitarios.

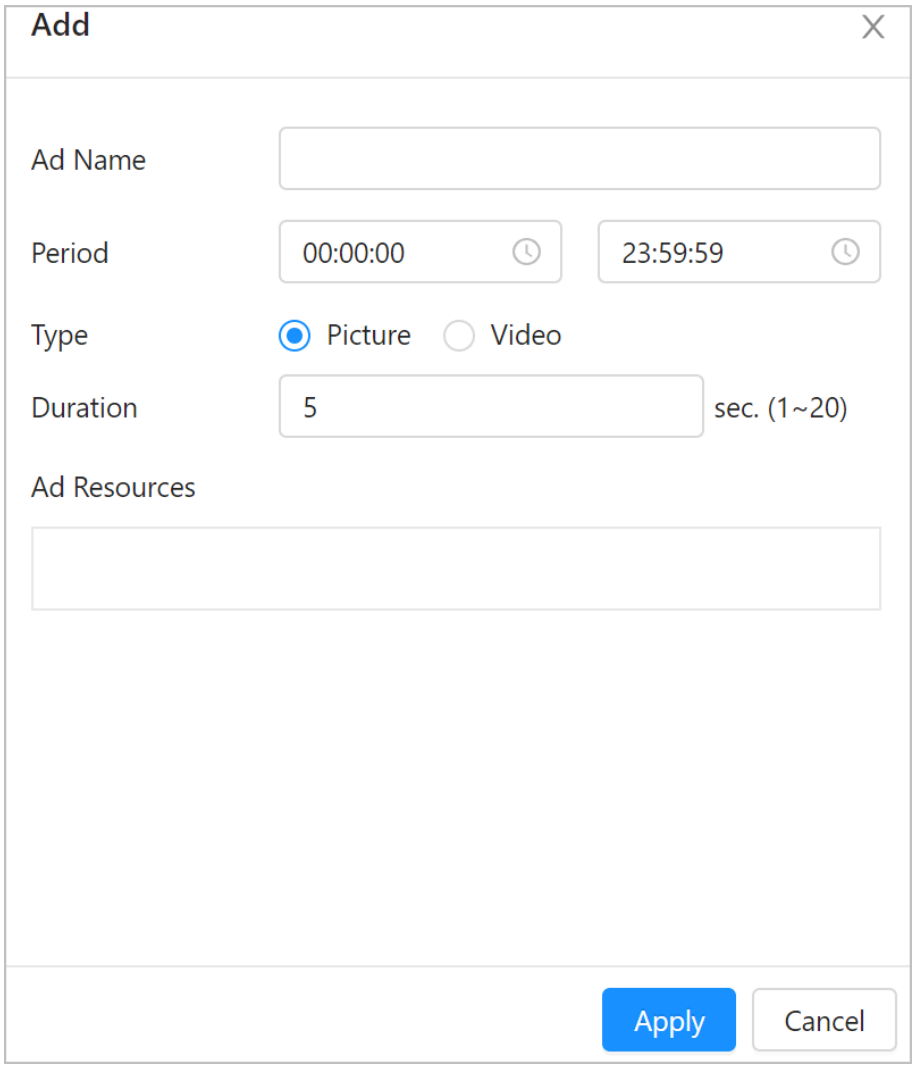
4) Seleccione el tipo de publicidad: Foto o video.

5) Establecer la duración de cada mago que se reproducirá.

6) Establecer recursos publicitarios.

7) Haga clic**Aplicar**.

Figura 6-14 Agregar planes de tiempo



Paso 5 Hacer clic**Aplicar**.

6.2.6.2 Configuración de textos publicitarios

Se conecta pantalla de matriz de puntos para mostrar textos publicitarios de la web. Paso

1 Seleccionar**General**>**Publicidad**>**Pantalla de matriz de puntos**.

Paso 2 Configuración de textos publicitarios.

Figura 6-15 Configurar textos publicitarios

Paso 3 Hacer clic**Aplicar**.

6.2.7 Bloqueo

Si el dispositivo está diseñado con cerradura electrónica, puede ir a**General**>**Cerrar**para desbloquear remotamente el compartimento superior o inferior.

En la página web, puede enviar comandos para bloquear o desbloquear el compartimento, pero no puede ver si el compartimento se cerró con éxito.

Figura 6-16 Configuración de bloqueo

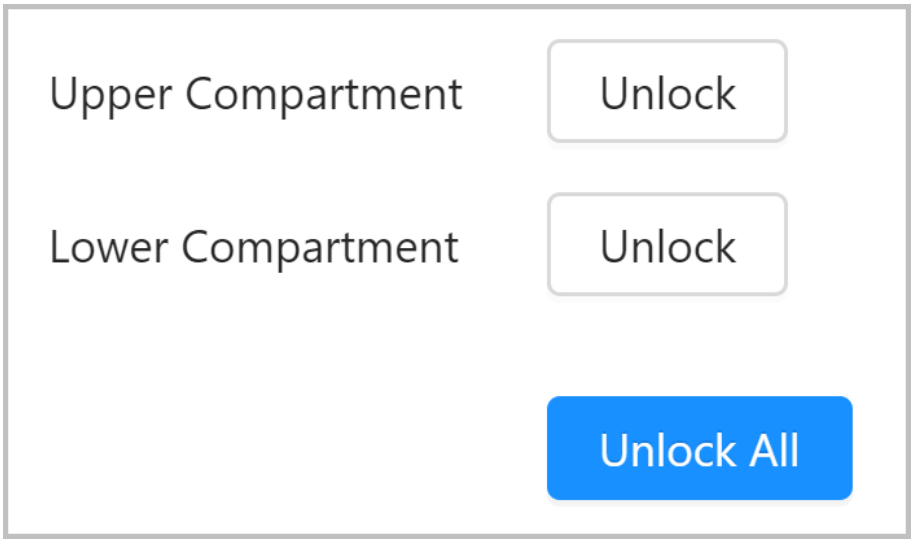


Tabla 6-7 Parámetros

Parámetros	Descripción
Compartimento Superior	Hacer clic**desbloquear**para desbloquear el compartimiento superior o inferior.
Compartimento Inferior	
Abrir todo	Hacer clic**Desbloquear todos**para desbloquear el compartimiento superior e inferior al mismo tiempo.

6.3 Red

Esta sección presenta la configuración de la red.

6.3.1 TCP/IP

requisitos previos

Asegúrese de que el dispositivo esté conectado a la red correctamente.

Puede configurar la dirección IP, el servidor DNS (Sistema de nombres de dominio) y más de acuerdo con el plan de red.

Procedimiento

Paso 1 Seleccionar**Red**>**TCP/IP**. Configure

Paso 2 los parámetros de TCP/IP.

Figura 6-17 Parámetros de TCP/IP

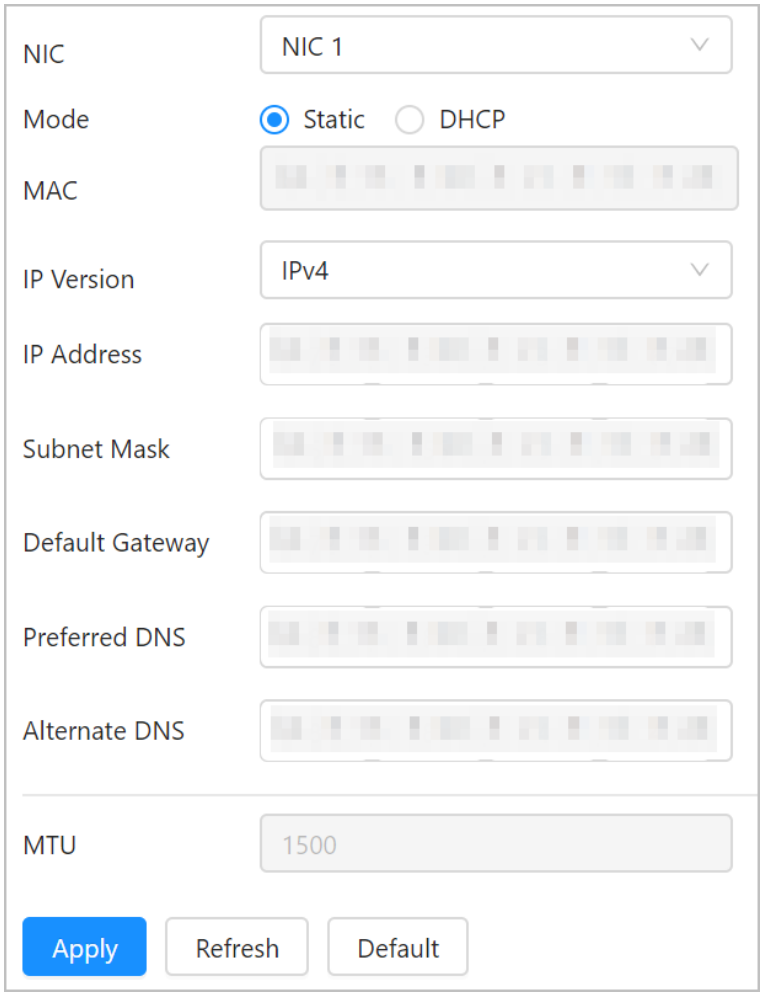


Tabla 6-8 Descripciones de los parámetros de TCP/IP

Parámetros	Descripción
NIC	Seleccionar**NIC1**o**NIC2**según las necesidades reales.
Modo	El modo en que el dispositivo obtiene IP: ● **Estático**: Configurar**Dirección IP**,**Máscara de subred**, y**Puerta de enlace predeterminada** manualmente y luego haga clic en**Ahorrar**, se muestra la página de inicio de sesión con la dirección IP configurada. ● **DHCP**(Protocolo de configuración de host dinámico): cuando hay un servidor DHCP en la red, seleccione**DHCP**y el dispositivo adquiere la dirección IP automáticamente.
Dirección MAC	Muestra la dirección MAC del host.
versión IP	Seleccionar**IPv4**o**IPv6**.
Dirección IP	cuando seleccionas**Estático**en**Modo**, ingrese la dirección IP y la máscara de subred que necesita. ● IPv6 no tiene máscara de subred. ● La puerta de enlace predeterminada debe estar en el mismo segmento de red con la dirección IP.
Máscara de subred	
Puerta de enlace predeterminada	

Parámetros	Descripción
DNS preferido	Dirección IP del DNS preferido y alternativo.
DNS alternativo	
MTU	El valor predeterminado es 1500.

Paso 3 Hacer clic**Aplicar**.

6.3.2 Puerto

Configure los números de puerto y la cantidad máxima de usuarios (incluye web, cliente de plataforma y cliente de teléfono móvil) que pueden acceder al dispositivo simultáneamente.

Paso 1 Seleccionar**Red**>**Puerto**. Configure

Paso 2 los parámetros del puerto.

Figura 6-18 Puerto

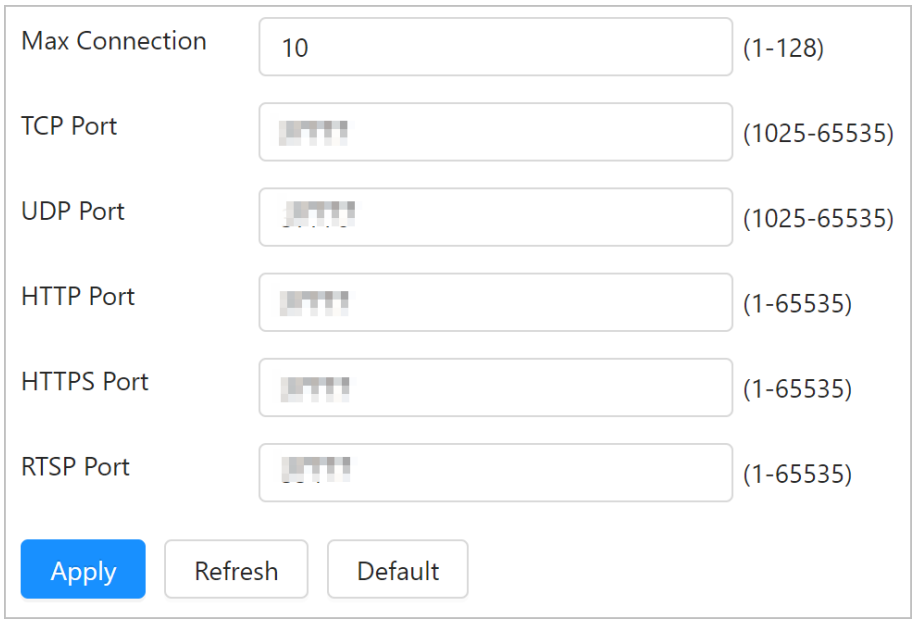


Tabla 6-9 Descripción de los parámetros del puerto

Parámetros	Descripción
Conexión máxima	El número máximo de usuarios (cliente web, cliente de plataforma o cliente de teléfono móvil) que pueden conectarse al dispositivo simultáneamente, el valor predeterminado es 10.
puerto TCP	Puerto de protocolo de control de transmisión. El valor es 37777 por defecto.
el puerto UDP	Puerto de protocolo de paquete de datos de usuario. El valor es 37778 por defecto.
puerto HTTP	Puerto de protocolo de transferencia de hipertexto. El valor es 80 por defecto.
puerto HTTPS	Puerto de comunicación HTTPS. Es 443 por defecto.

Parámetros	Descripción
Puerto RTSP	● Puerto de protocolo de transmisión en tiempo real, y el valor es 554 por defecto. Si juega en vivo con QuickTime, VLC o un teléfono inteligente Blackberry, el siguiente formato de URL está disponible. Si juegas en vivo con QuickTime de Safari o VLC, el siguiente formato de URL está disponible. ● Cuando el formato de URL requiere RTSP, debe especificar el número de canal y el tipo de flujo de bits en la URL, y también el nombre de usuario y la contraseña, si es necesario. ● Al reproducir la vista en vivo con el teléfono inteligente Blackberry, debe apagar el audio y luego configurar el modo de código en H.264B y la resolución en CIF. Ejemplo de formato de URL: rtsp://nombre de usuario:@ IP Dirección: puerto/cámara/realmonitor?channel=1&subtype=0 Si el nombre de usuario y la contraseña no son necesarios para la verificación, la URL puede ser: rtsp://ip:puerto/cámara/realmonitor?channel=1&subtype=0 ● Nombre de usuario: admin, por ejemplo. ● Contraseña: Su contraseña. Por ejemplo, administrador. ● IP: IP del dispositivo. Por ejemplo, 192.168.1.122. ● Puerto: Déjalo si el valor por defecto es 554. ● Canal 1: número de canal, comienza desde 1. Por ejemplo, si está utilizando el canal 2, canal = 2 ● Subtipo: el tipo de flujo de bits; 0 significa transmisión principal (Subtipo=0) y 1 significa transmisión secundaria (Subtipo=1). Ejemplo: si necesita la transmisión secundaria del canal 2 desde un determinado dispositivo, entonces la URL debe ser: rtsp://administrador: admin@192.168.1.123 :554/cam/realmonitor?channel=2 &subtype=1

Paso 3 Hacer clic**Aplicar**.

6.3.3 2G/4G

requisitos previos

Asegúrese de que se haya instalado el módulo 2G/4G

Información de contexto

Conecte el dispositivo a una red 2G/4G a través del método de acceso telefónico de diferentes operadores. Luego puede recibir información sobre alarmas y el estado de los dispositivos en su dispositivo móvil.

Procedimiento

Paso 1 Seleccionar**Red**>**2G/4G**.

Paso 2 Hacer clic junto a**Permitir**y**Marcar**para habilitar el 2G/4G y la función de marcación.

Figura 6-19 Configuración 2G/4G

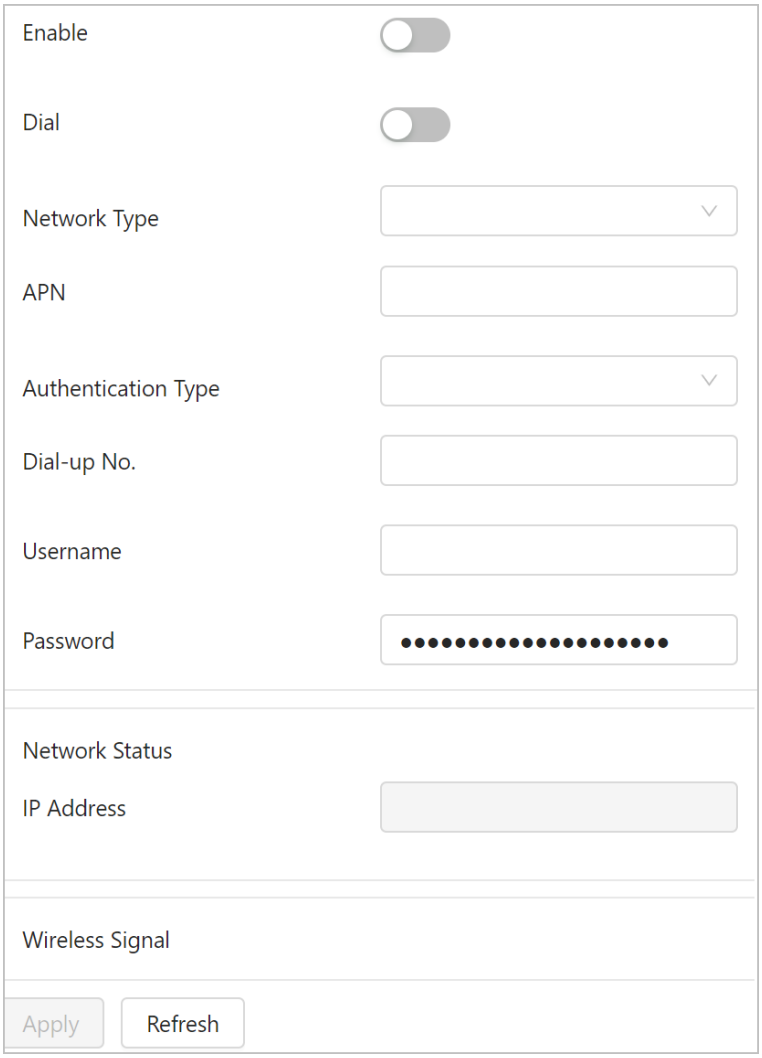


Tabla 6-10 Descripciones de parámetros 2G/4G

Parámetros	Descripción
Tipo de red	Seleccionar**WCDMA**,**Auto**,**EVDO**,**TD-SCDMA**,**TD-LTE** y**FDD-LTE**.
APN	Muestra el punto de acceso del operador de comunicación.
tipo de autenticación	Cuando está habilitado, el sistema reconoce automáticamente el protocolo, incluyendo**PAPILLA**,**CAP**y**NO**.
número de acceso telefónico	Introduzca el número de marcación proporcionado por el operador de comunicación.
Nombre de usuario	El dispositivo completa la información de marcación automáticamente después de reconocer el módulo 2G/4G.
Contraseña	
Estado de la red	Muestra el estado de conexión de la red.
Dirección IP	Después de que la conexión a la red sea exitosa, el dispositivo obtendrá y mostrará la dirección IP automáticamente.
señal inalámbrica	La intensidad de la señal actual del dispositivo.

Paso 3 Hacer clic**Aplicar**.

6.3.4 UPnP

requisitos previos

- Asegúrese de que el servicio UPnP esté instalado en el sistema.
- Inicie sesión en el enrutador y configure la dirección IP de WAN para configurar la conexión a Internet.
- Habilitar UPnP en el enrutador
- Conecte su dispositivo al puerto LAN del enrutador.
- Seleccionar**Red**>**TCP/IP**, ingrese la dirección IP del área local del enrutador o seleccione**DHCP**y adquiere la dirección IP automáticamente.

Información de contexto

UPnP (Universal Plug and Play) es un protocolo que establece una relación de mapeo entre las redes de área local y de área amplia. Esta función le permite acceder al dispositivo de área local a través de una dirección IP de área amplia.

Procedimiento

Paso 1 Seleccionar**Red**>**UPnP**.

Paso 2 Hacer clic para habilitar la función UPnP.

Paso 3 Seleccione un servicio y haga clic en para habilitar la función de servicio.

Etapa 4 Haga clic para modificar el número de puerto externo correspondiente y luego haga clic en**DE ACUERDO**. Hacer clic

Paso 5 **Aplicar**.

6.3.5 Registro

Después de habilitar esta función, cuando el dispositivo esté conectado a Internet, informará la ubicación actual al servidor especificado que actúa como tránsito para facilitar que el software del cliente acceda al dispositivo.

Paso 1 Seleccionar**Red**>**Registro**. Hacer

Paso 2 clic para habilitar la función de registro.

Paso 3 Ingrese la dirección del servidor, el puerto y la ID del subdispositivo.

Figura 6-20 Registro

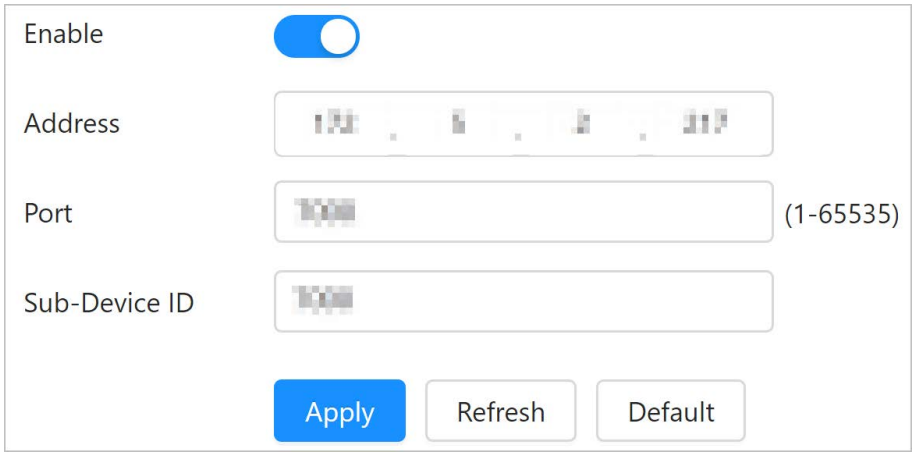


Tabla 6-11 Parámetros de registro

Parámetros	Descripción
DIRECCIÓN	La dirección IP o nombre de dominio del servidor a registrar.
Puerto	El puerto para el registro.
ID de subdispositivo	El ID personalizado para el dispositivo.

Etapa 4 Hacer clic**Aplicar**.

6.3.6 Servidor SIP

Con SIP (Protocolo de inicio de sesión), el dispositivo se puede registrar en la plataforma. Cuando presiona el botón de alarma, puede tener una conversación de voz y video en la plataforma.

Paso 1 Seleccionar**Red**>**Servidor SIP**.

Paso 2 Ingrese la dirección IP del servidor, el puerto, el nombre de usuario, la contraseña, el dominio SIP y el ID de llamada del dispositivo.

Figura 6-21 Configurar servidor SIP

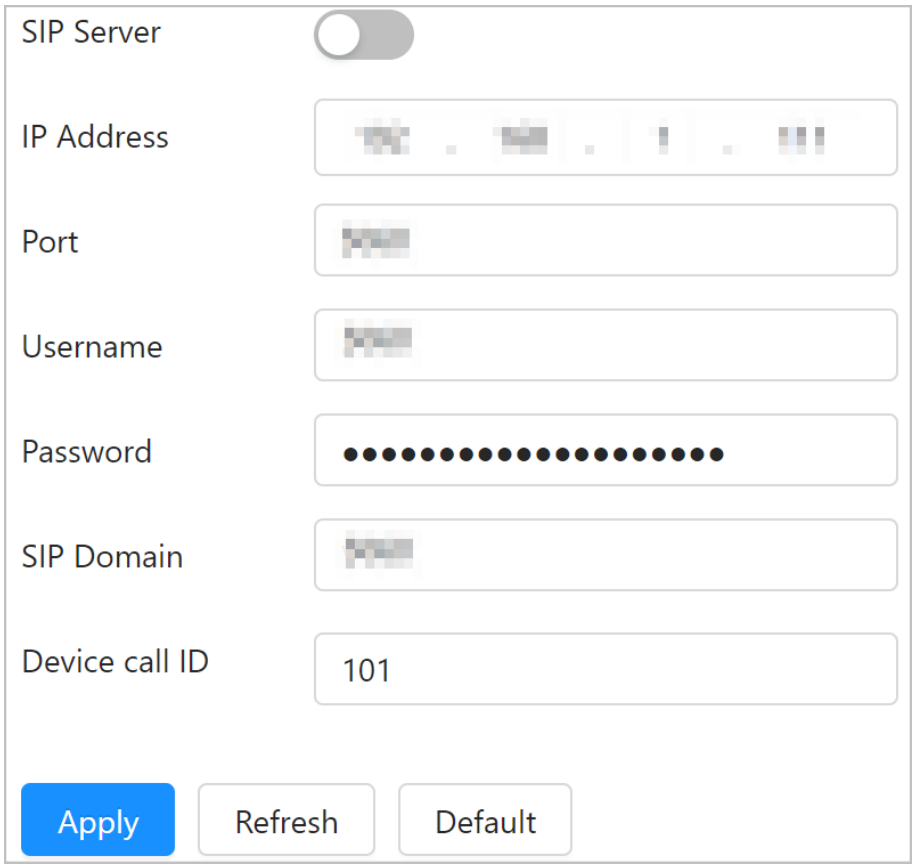


Tabla 6-12 Descripciones de los parámetros del servidor SIP

Parámetros	Descripción
Servidor SIP	Si la plataforma funciona como servidor SIP, ingrese la dirección IP de la plataforma.
Dirección IP	
Puerto	Si la plataforma funciona como servidor SIP, ingrese 5080 en el puerto del servidor SIP.
Nombre de usuario	Nombre de usuario para acceder al servidor SIP.
Contraseña	La contraseña para acceder al servidor SIP.
Dominio SIP	Si la plataforma funciona como servidor SIP, mantenga el valor nulo.
ID de llamada del dispositivo	El número de ID del dispositivo al que se llama.

Paso 3 Hacer clic para habilitar la función de servidor SIP.

Etapa 4 Hacer clic**Aplicar**.

6.3.7 FTP

Puede almacenar y ver los videos grabados y las instantáneas en el servidor FTP.

Seleccionar**Sistema**>**Almacenamiento**y, a continuación, establezca Método de almacenamiento en**FTP**, después de lo cual puede almacenar el videos grabados e instantáneas

Paso 1 Seleccionar**Red**>**FTP**.

Paso 2 Configure los parámetros.

Figura 6-22 FTP

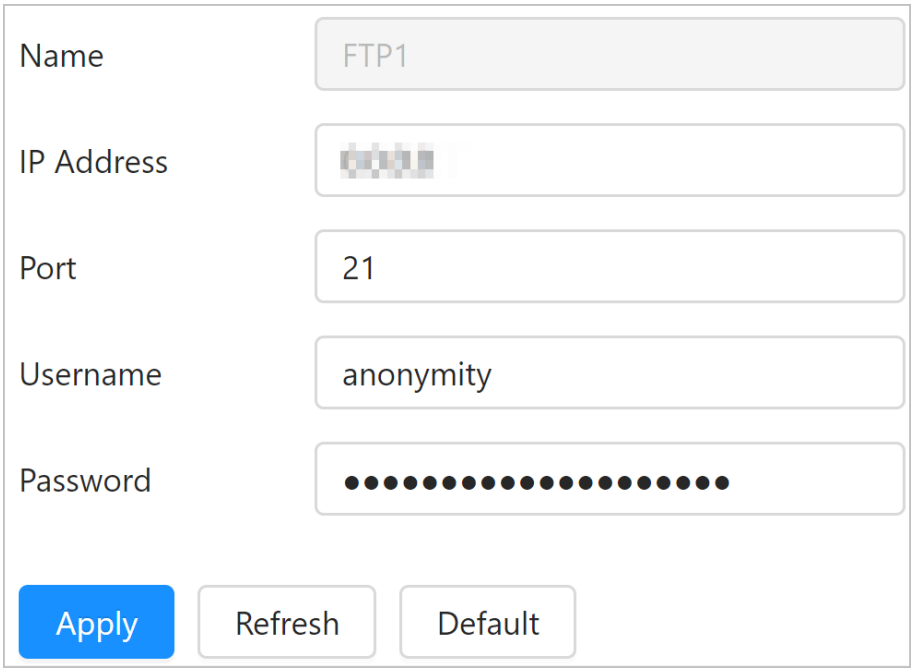


Tabla 6-13 Descripciones de los parámetros de FTP

Parámetros	Descripción
Dirección IP	Dirección IP de la PC que está instalada con el servidor FTP.
Puerto	El número de puerto del servidor FTP.
Nombre de usuario	Nombre de usuario y contraseña para acceder al servidor FTP.
Contraseña	

Paso 3 Hacer clic**Aplicar**.

6.3.8 Servicios básicos

Configure los hosts IP (dispositivos con dirección IP) que pueden visitar el dispositivo. Solo los hosts en la lista de sitios confiables pueden iniciar sesión en la página web. Esto es para mejorar la red y la seguridad de los datos. Paso 1 Seleccionar**Red**>**Servicios basicos**. Hacer

Paso 2 clic para habilitar el servicio básico de acuerdo a las necesidades reales.

Figura 6-23 Servicios básicos

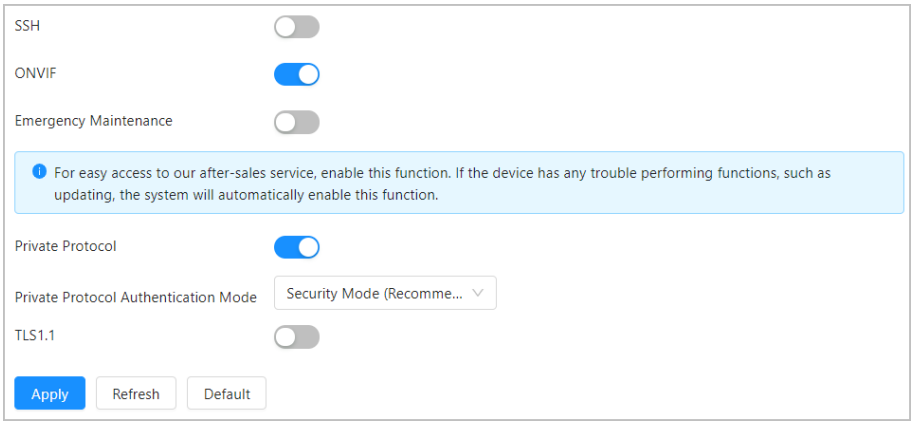


Tabla 6-14 Descripciones de los parámetros básicos del servicio

Parámetros	Descripción
SSH	Puede habilitar la autenticación SSH (Secure Shell) para realizar la gestión de seguridad. La función está deshabilitada por defecto.
ONVIF	Habilitado por defecto. El dispositivo puede conectarse con otros productos de video en red a través de este protocolo.
Emergencia Mantenimiento	Para acceder fácilmente a nuestro servicio posventa, habilite la función de mantenimiento de emergencia. Si el dispositivo tiene problemas para realizar funciones, como la actualización, el sistema habilitará automáticamente esta función.
Protocolo privado	Habilitado por defecto. Seleccione el modo de autenticación de**modo de seguridad**y**Modo compatible**.**modo de seguridad**es recomendado.
Protocolo privado modo de autenticación	
TSL1.1	Si está habilitado,**TLS1.1**y**TLS1.2**son compatibles. Si está deshabilitado, solo**TLS1.2** esta apoyado.

Paso 3 Hacer clic**Aplicar**.

6.4 Sistema

Esta sección presenta las configuraciones del sistema, incluidas las generales, fecha y hora, administración de usuarios, mantenimiento y más.

6.4.1 Cuenta

Puede administrar usuarios, como agregarlos, eliminarlos o editarlos. Los usuarios incluyen administradores, usuarios agregados y usuarios de ONVIF.

Solo los administradores pueden administrar usuarios y grupos.

- Se pueden agregar hasta 64 usuarios (el usuario administrador no está incluido) y hasta 20 grupos de usuarios (el grupo con el usuario administrador no está incluido).
- Puede administrar usuarios a través de usuarios o grupos de usuarios, no se permite el mismo nombre de usuario o nombre de grupo. Un usuario debe pertenecer a 1 grupo a la vez, y los usuarios de un grupo solo han definido

autoridades asociadas al grupo.

- Los usuarios en línea no pueden modificar sus propias autoridades.
- Hay un administrador por defecto que tiene las autoridades más altas.

6.4.1.1 Agregar usuario

Eres usuario administrador por defecto. Puede agregar usuarios y configurar diferentes permisos.

Procedimiento

Paso 1 Seleccionar**Sistema**>**Cuenta**>**Usuario**. Hacer

Paso 2 clic**Agregar**.

Paso 3 Configurar parámetros de usuario.

Figura 6-24 Agregar usuarios

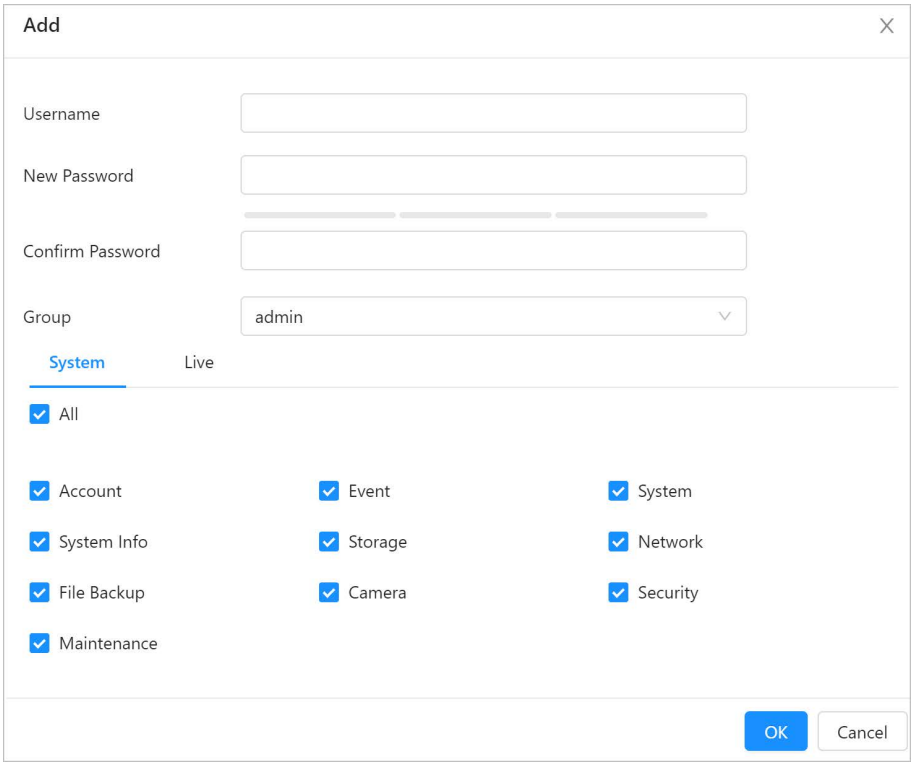


Tabla 6-15 Descripciones de parámetros de usuario

Parámetros	Descripción
Nombre de usuario	Identificación única del usuario. No puede utilizar un nombre de usuario existente. El nombre de usuario puede contener 31 caracteres, incluidos números, letras, subrayados, guiones, puntos y @.
Nueva contraseña	Introduzca la contraseña y confírmela de nuevo. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &).
Confirmar Contraseña	
Grupo	El grupo al que pertenecen los usuarios. Cada grupo tiene diferentes autoridades.

Parámetros	Descripción
MAC	Introduzca la dirección MAC. Cuando ingrese la dirección MAC, solo la computadora de la dirección MAC puede acceder al dispositivo.
Sistema	Seleccione las autoridades según sea necesario. Recomendamos otorgar menos permisos a los usuarios normales que a los usuarios premium.
Vivir	Seleccione la autoridad de visualización en vivo para que se agregue el usuario.

Etapa 4 Hacer clic**DE ACUERDO**.

Los usuarios recién agregados se muestran en la lista de usuarios.

Operaciones relacionadas

- Modificación de la información del usuario

  Haga clic para editar la contraseña, el grupo, la nota o las autoridades.

  Para la cuenta de administrador, solo puede cambiar la contraseña.

- Eliminación de usuario

  Haga clic para eliminar los usuarios agregados.

  El usuario administrador no se puede eliminar.

6.4.1.2 Agregar grupo de usuarios

Tiene dos grupos llamados administrador y usuario de forma predeterminada, y puede agregar un nuevo grupo, eliminar un grupo agregado o editar la autoridad y la nota del grupo.

Procedimiento

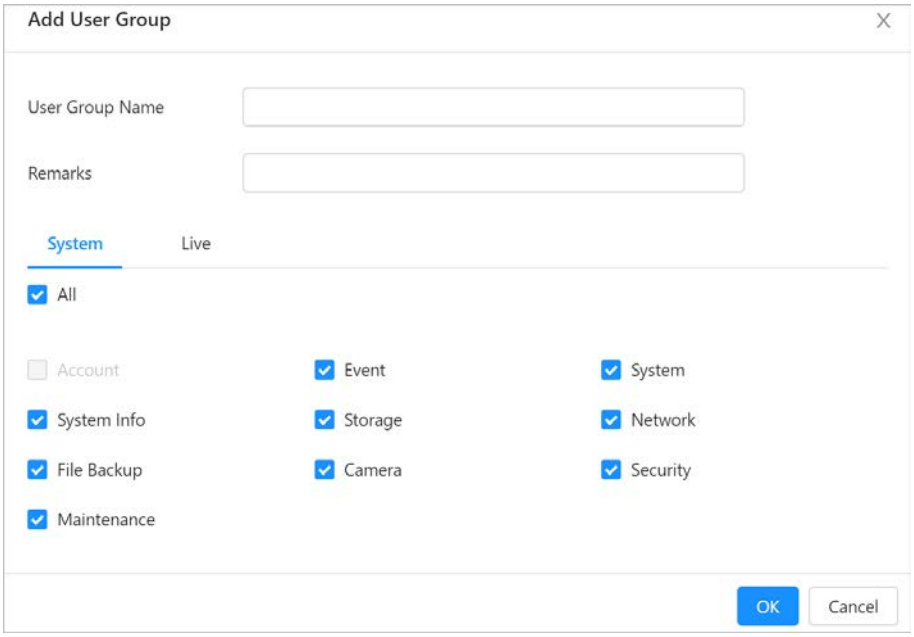
Paso 1 Seleccionar**Sistema**>**Cuenta**>**Grupo**. Hacer

Paso 2 clic**Añadir grupo**.

Paso 3 Ingrese el nombre del grupo y los comentarios, y luego seleccione las autoridades del grupo.

El nombre de usuario puede contener 31 caracteres, incluidos números, letras, subrayados, guiones, puntos y @.

Figura 6-25 Agregar grupos de usuarios



Etapa 4 Hacer clic**DE ACUERDO**.

El grupo recién agregado se muestra en la lista de grupos.

Operaciones relacionadas

- Modificación de la información del grupo de usuarios

  Haga clic para editar la contraseña, el grupo, los comentarios o las autoridades.

- Eliminación de un grupo de usuarios

  Haga clic para eliminar los grupos de usuarios agregados.

  El grupo de administradores y el grupo de usuarios no se pueden eliminar.

6.4.1.3 Usuario ONVIF

Puede agregar, eliminar usuarios de ONVIF y modificar sus contraseñas.

Procedimiento

Paso 1 Seleccionar**Sistema**>**Cuenta**>**Usuario ONVIF**. Hacer

Paso 2 clic**Agregar**.

Paso 3 Configurar parámetros.

Figura 6-26 Agregar usuarios ONVIF

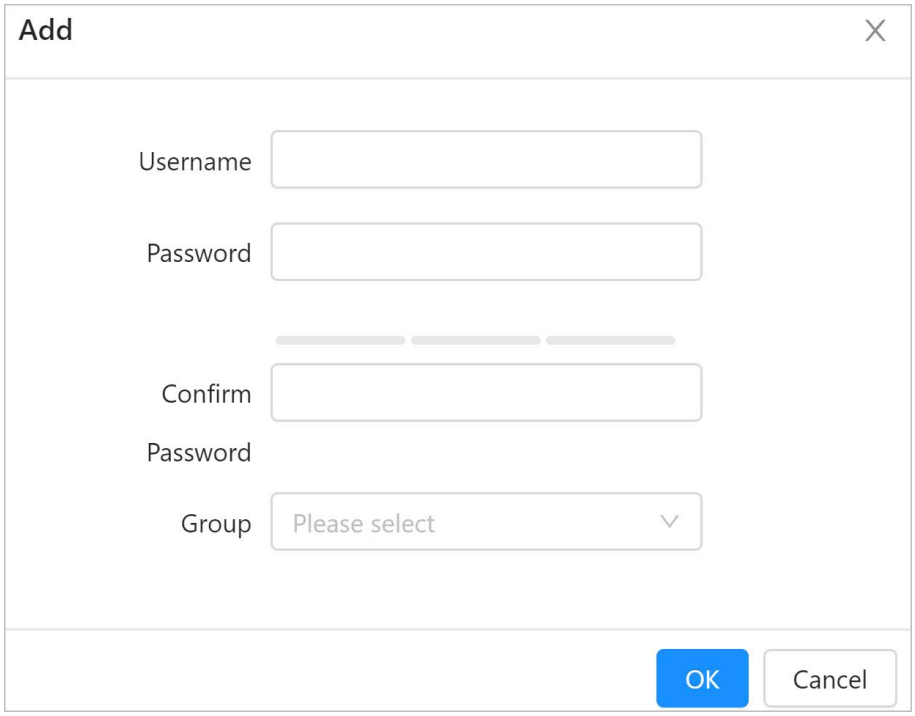


Tabla 6-16 Descripciones de los parámetros de usuario de ONVIF

Parámetros	Descripción
Nombre de usuario	Identificación única del usuario. No puede utilizar un nombre de usuario existente. El nombre de usuario puede contener 31 caracteres, incluidos números, letras, subrayados, guiones, puntos y @.
Contraseña	Introduzca la contraseña y confírmela de nuevo. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &).
Confirmar Contraseña	
Grupo	El grupo al que pertenecen los usuarios. Cada grupo tiene diferentes autoridades.

Etapa 4 Hacer clic**DE ACUERDO**.

El usuario recién agregado se muestra en la lista de usuarios.

Operaciones relacionadas

- Modificación de la información del usuario

  Haga clic para editar la contraseña, el grupo, los comentarios o las autoridades.

  Para la cuenta de administrador, solo puede cambiar la contraseña.

- Eliminación de usuario

  Haga clic para eliminar los usuarios agregados.

  La cuenta de administrador no se puede eliminar.

6.4.2 Tiempo

Configure la fecha y la zona horaria, DST y otros parámetros del dispositivo.

Paso 1 Seleccionar**Sistema**>**Tiempo**. Configure los

Paso 2 parámetros de fecha y hora.

Figura 6-27 Ajustes de tiempo

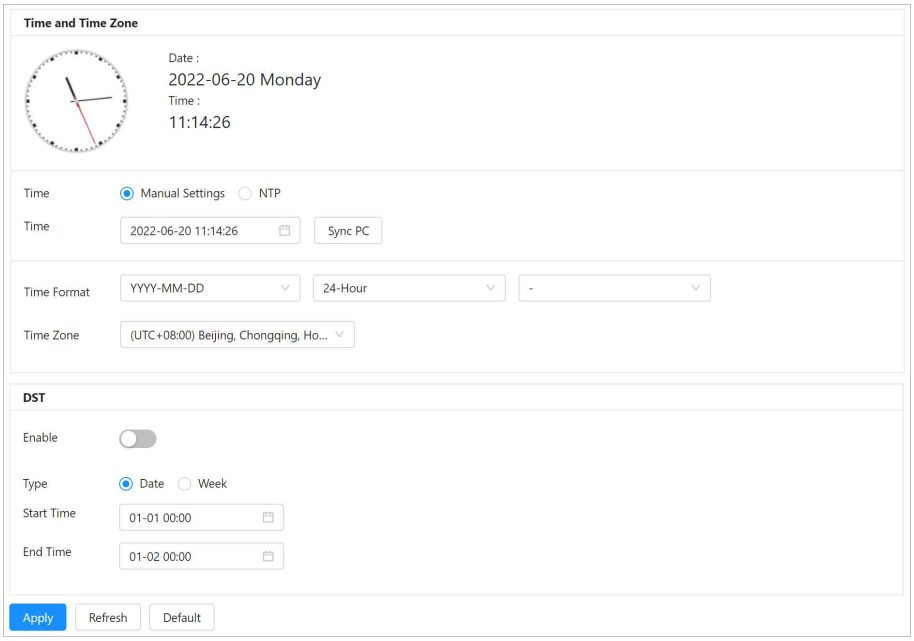


Tabla 6-17 Descripciones de los parámetros de fecha y hora

Parámetros	Descripción
Tiempo	Seleccionar**Ajustes manuales**o**NTP**. ● **Configuración manual**: Configure los parámetros manualmente. Hacer clic**Sincronizar PC**para sincronizar con la hora de la computadora. ● **NTP**: Al seleccionar NTP, el sistema sincroniza la hora con el servidor de Internet en tiempo real. También puede ingresar la dirección IP, la zona horaria, el puerto y el intervalo de una PC que instaló el servidor NTP para usar NTP. ◇ **Servidor**: Haga clic**Actualización manual**para sincronizar la hora con el servidor de internet en tiempo real. ◇ **Puerto**: El sistema solo admite el protocolo TCP y la configuración predeterminada es 123 (1–65535). ◇ **Intervalo**: Ingrese el intervalo en el que desea que el dispositivo sincronice la hora desde el servidor NTP. El valor máximo es 65535 minutos.
Formato de tiempo	● Seleccione un formato de fecha, incluyendo**AAAA-MM-DD**,**MM-DD-AAAA**, y**DD-MM-AAAA**. ● Seleccionar**24 horas**o**12 horas**.
Zona horaria	Seleccione según la ubicación del dispositivo.

Parámetros	Descripción
horario de verano	Algunos países o regiones implementan el horario de verano. Seleccione si habilitar el horario de verano del dispositivo según las necesidades reales. 1. Haga clic en para habilitar la función DST. 2. Selecciona**Tipo**de**Fecha**o**Semana**. 3. Establezca la hora de inicio y la hora de finalización del horario de verano.

Paso 3 Hacer clic**Aplicar**.

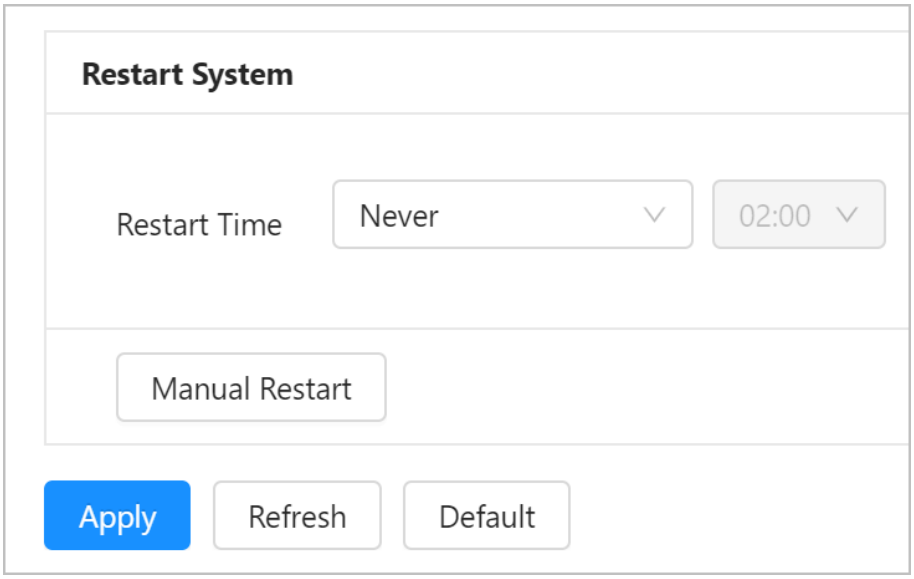
6.4.3 Mantenimiento

6.4.3.1 Mantenimiento automático

Puede reiniciar el sistema manualmente y establecer la hora de reinicio automático.

Paso 1 Seleccionar**Sistema**>**Mantenimiento**>**Mantenimiento automático**.

Figura 6-28 Mantenimiento automático



Paso 2 Reinicie el dispositivo.

- En el**Reiniciar sistema**área, configure el tiempo de reinicio, y luego el sistema se reiniciará automáticamente a la hora definida cada semana.
- Hacer clic**Reinicio manual**, y luego el dispositivo se reinicia inmediatamente. Hacer

Paso 3 clic**Aplicar**.

6.4.3.2 Configuración de ajustes de copia de seguridad

Importe o exporte archivos de configuración del sistema y haga una copia de seguridad de ellos cuando varios dispositivos utilicen los archivos de configuración.

Paso 1 Seleccionar**Sistema**>**Mantenimiento**>**Copia de seguridad de configuración**

Paso 2 . Importar o exportar el archivo.

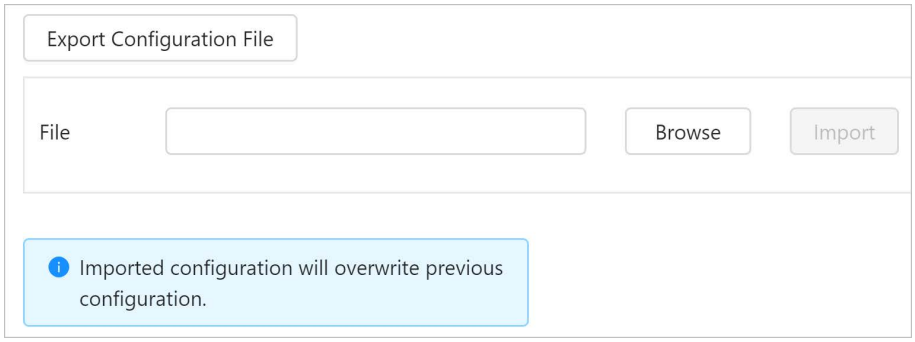
- Exportar información de configuración.

  Hacer clic**Exportar archivo de configuración**para exportar el archivo de configuración del sistema al almacenamiento local.

- Importar archivo de configuración

  Hacer clic**Navegar**, seleccione el archivo de configuración local y haga clic en**Importar archivo**para importar el archivo de configuración del sistema local al sistema.

Figura 6-29 Copia de seguridad



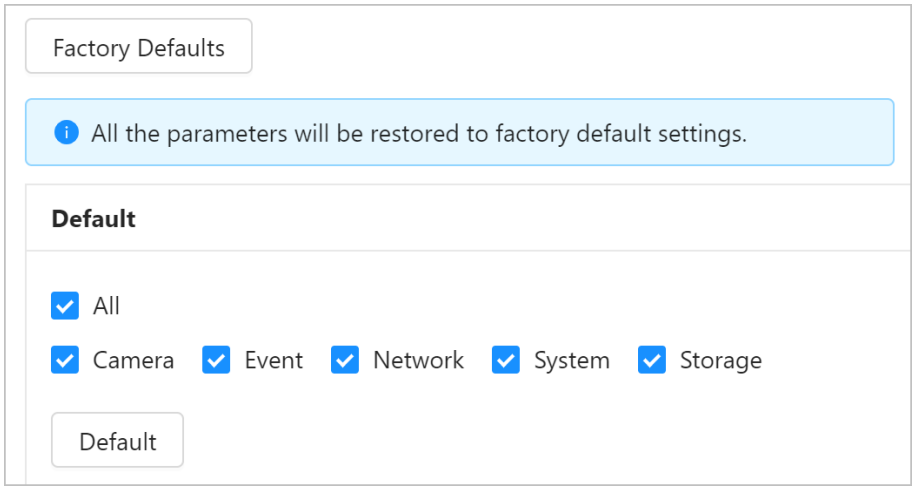
6.4.3.3 Predeterminado

Restaure el dispositivo a la configuración predeterminada o a la configuración de fábrica.

La operación borrará los datos del dispositivo. Ser cauteloso.

- Hacer clic**Fallas de fábrica**, y luego todas las configuraciones excepto la dirección IP y la cuenta se restablecen a los valores predeterminados.
- Hacer clic**Por defecto**, y todas las configuraciones se restablecen a los valores de fábrica.

Figura 6-30 Predeterminado



6.4.4 Actualizar

- Durante la actualización, no desconecte la fuente de alimentación, la red y no reinicie ni apague el dispositivo.
- Seleccione los archivos de actualización correctos; de lo contrario, es posible que algunas funciones no funcionen correctamente.

Paso 1 Seleccionar**Sistema**>**Actualizar**.

Paso 2 Configurar parámetros.

Paso 3 Hacer clic**Navegar**y, a continuación, seleccione el archivo de actualización (archivo .bin) que desea importar.

Etapa 4 Hacer clic**Actualizar**para actualizar el sistema.

El dispositivo se reinicia después de completar la actualización.

6.4.5 Almacenamiento

Seleccionar**Sistema**>**Almacenamiento**y luego vea la información de la tarjeta SD local, formatee la tarjeta SD y configure el método de almacenamiento para los videos grabados.

Para los métodos de almacenamiento, puede seleccionar**Dakota del Sur**o**FTP**.

- **Dakota del Sur**: Guarde los videos grabados en la tarjeta SD interna.
- **FTP**: Guarde los videos grabados en el servidor FTP.

6.5 Información del sistema

6.5.1 Versión

Seleccionar**Información del sistema**>**Versión**para ver la información del dispositivo, como el hardware, la versión del sistema y la versión web.

6.5.2 Información legal

Seleccionar**Información del sistema**>**Información legal**para ver el acuerdo de licencia de software, la política de privacidad y el aviso de software de código abierto.

6.6 Registros

6.6.1 Visualización del historial de llamadas

Seleccionar**Registro**>**Historial de llamadas**para ver el historial de llamadas, incluidos los tipos de llamadas y el número de teléfono.

6.6.2 Visualización de registros

El tipo de registro incluye Todo, Sistema, Usuario, Configuración, Evento, Operación y Seguridad.

- **Sistema**: Incluye inicio de programa, cierre anormal, cierre, reinicio de programa, cierre de dispositivo, reinicio de dispositivo, reinicio de sistema y actualización de sistema.
- **Usuario**: incluye inicio de sesión, cierre de sesión, adición de usuario, eliminación de usuario, edición de usuario, adición de grupo, eliminación de grupo y edición de grupo.
- **Configuración**: incluye guardar configuración, eliminar archivo de configuración, acceso a archivo, error de acceso a archivo y búsqueda de archivo.
- **Evento**(registra eventos como detección de video, plan inteligente, alarma y anormalidad): incluye el inicio y el final del evento.
- **Operación**: incluye la configuración del tipo de disco, el borrado de datos, el intercambio en caliente, el estado de FTP y el modo de grabación.

- **Seguridad**: Incluye restablecimiento de contraseña y filtro de IP.

Paso 1 Seleccionar**Registro**>**Registro**.

Paso 2 Establezca la hora de inicio y la hora de finalización, y luego seleccione los tipos de registro.

Paso 3 Hacer clic**Buscar**.

- Hacer clic o haga clic en un determinado registro, y luego podrá ver la información detallada.
- Hacer clic**Respaldo**, y luego puede hacer una copia de seguridad de todos los registros de búsqueda en la PC local.

Si desea cifrar los registros, puede seleccionar**Cifrar copia de seguridad de registros**, introducir la contraseña, y luego haga clic**Respaldo**.

6.6.3 Visualización de registros remotos

Configure el registro remoto y podrá obtener el registro relacionado accediendo a la dirección establecida. Paso 1 Seleccionar**Registro**>**Registro remoto**.

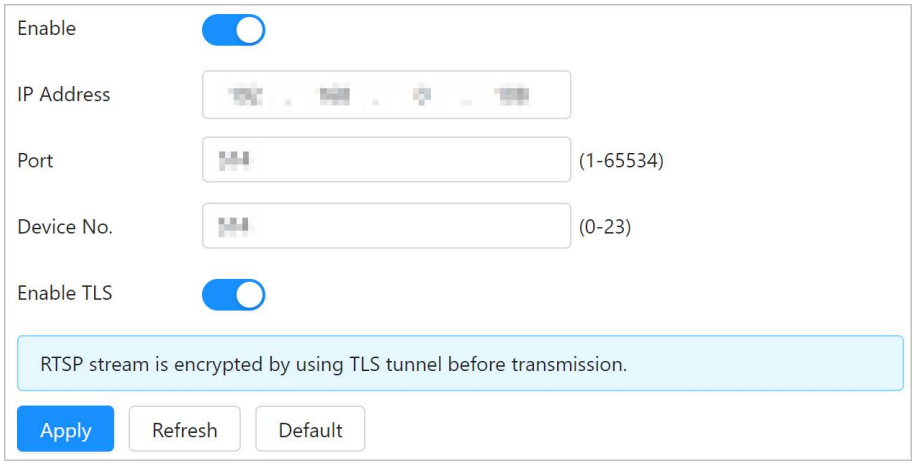
Paso 2 Hacer clic para permitir**Registro remoto**función.

Paso 3 Configure la dirección IP, el puerto y el número de dispositivo del servidor remoto.

Etapa 4 Hacer clic para permitir**TLS**función.

Paso 5 Hacer clic**Aplicar**.

Figura 6-31 Registro remoto



6.7 Seguridad

6.7.1 Estado de seguridad

Información de contexto

Detecte al usuario y el servicio, y escanee los módulos de seguridad para verificar el estado de seguridad de la cámara, de modo que cuando aparezca una anomalía, pueda procesarla a tiempo.

- Detección de usuarios y servicios: detecte la autenticación de inicio de sesión, el estado del usuario y la seguridad de la configuración para verificar si la configuración actual cumple con las recomendaciones.
- Escaneo de módulos de seguridad: escanee el estado de funcionamiento de los módulos de seguridad, como transmisión de audio/video, protección confiable, advertencia de seguridad y defensa contra ataques, no detecte si

están habilitados.

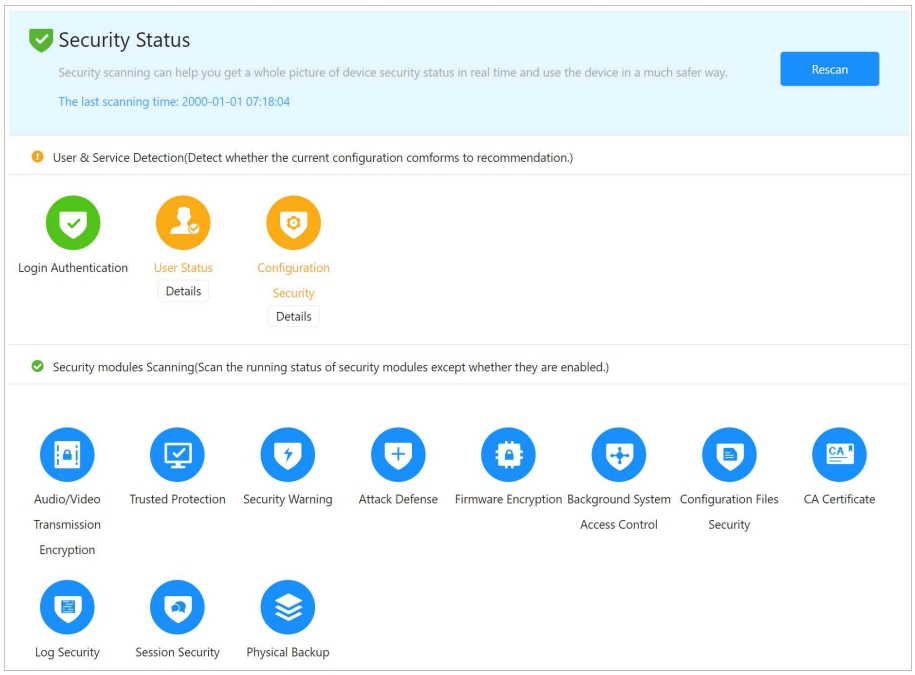
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Estado de seguridad**.

Paso 2 Hacer clic**volver a escanear**para escanear el estado de seguridad del dispositivo.

Durante el escaneo, el ícono se vuelve gris. Cuando se completa el escaneo, el ícono se vuelve azul.

Figura 12-1 Estado de seguridad



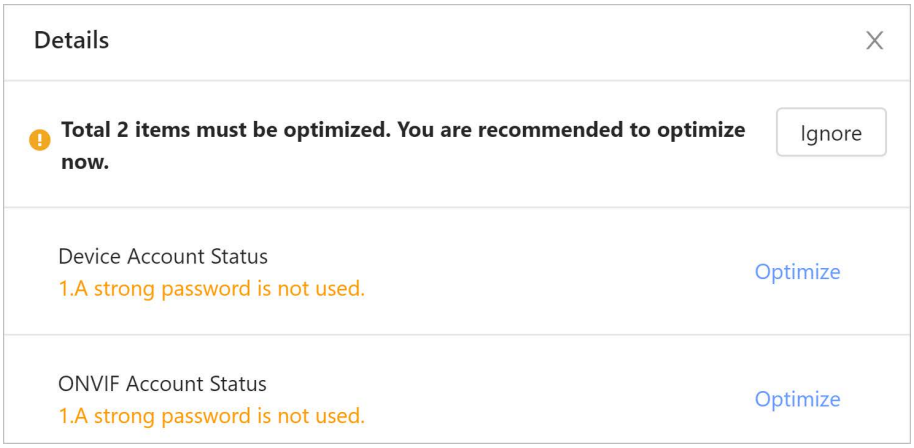
Operaciones relacionadas

Después de escanear, se mostrarán diferentes resultados con diferentes colores. El amarillo indica que los módulos de seguridad son anormales y el verde indica que los módulos de seguridad son normales.

- Hacer clic**Detalles**para ver los detalles del resultado del escaneo.
- Hacer clic**Ignorar**para ignorar la excepción, y no se escaneará en el próximo escaneo.

  Hacer clic**Detección conjunta**, y la excepción se escaneará en el siguiente escaneo.
- Hacer clic**Optimizar**, y se muestra la página correspondiente, y puede editar la configuración para borrar la excepción

Figura 12-1 Ver detalles



6.7.2 Servicio del sistema

Solo cuando la función de servicio del sistema está habilitada, puede usar la función correspondiente.

6.7.2.1 802.1x

El dispositivo puede conectarse a la LAN después de pasar la autenticación 802.1x. Tanto el conmutador como el dispositivo deben pasar la autenticación 802.1x; de lo contrario, no podrá acceder al dispositivo a través de la red.

Paso 1 Seleccionar**Seguridad**>**Servicio del sistema**>**802.1x**. Seleccione el

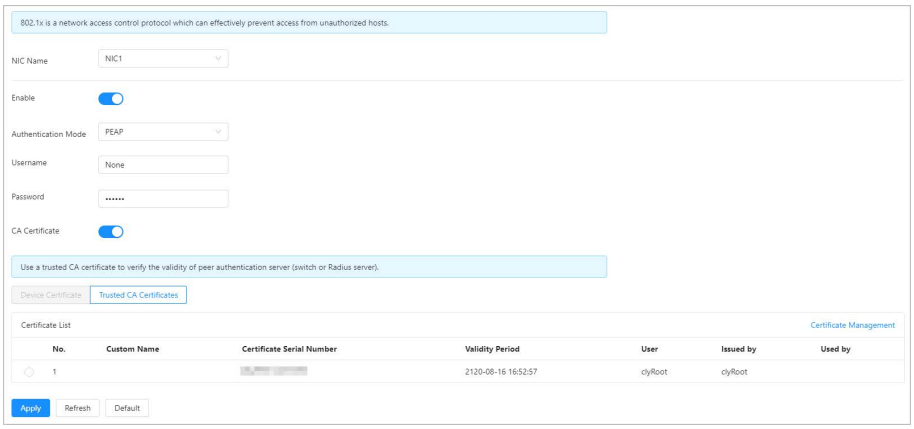
Paso 2 nombre de la NIC según sea necesario y haga clic en para habilitarlo.

Paso 3 Seleccione el modo de autenticación y luego configure los parámetros.

- **PEAP**: Protocolo EAP protegido.
  1. Seleccione**PEAP**como modo de autenticación.
  2. Introduzca el nombre de usuario y la contraseña que se ha autenticado en el servidor.
  3. Haga clic en junto al certificado de CA y seleccione el certificado de CA de confianza en la lista.

  Si no hay ningún certificado en la lista, haga clic en**Gestión de certificados**A la izquierda barra de navegación. Para obtener más información, consulte "6.7.4.2 Instalación del certificado de CA de confianza".

Figura 12-1 802.1x(PEAP)

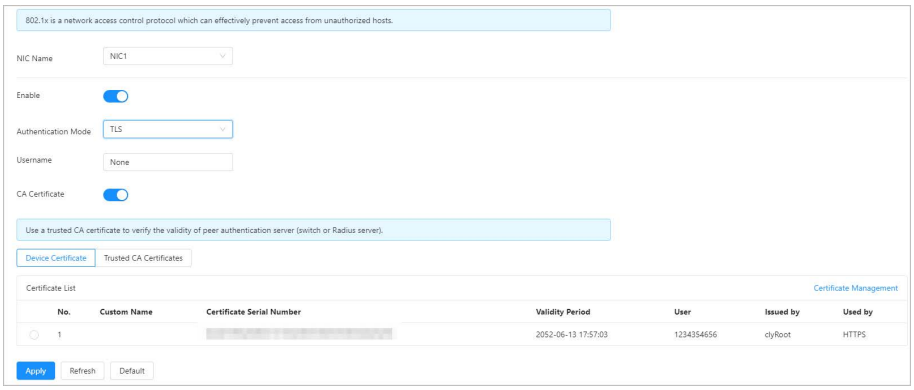


- **TLS**: TLS: Seguridad de la capa de transporte. Se aplica en dos programas de aplicación de comunicación para garantizar la seguridad e integridad de los datos.

1. Seleccione**TLS**como modo de autenticación.
2. Introduzca el nombre de usuario.
3. Haga clic en junto al certificado de CA y seleccione el certificado de CA de confianza en la lista.

Si no hay ningún certificado en la lista, haga clic en**Gestión de certificados**A la izquierda barra de navegación. Para obtener más información, consulte "6.7.4.2 Instalación del certificado de CA de confianza".

Figura 12-1 802.1x (TLS)



Etapa 4 Hacer clic**Aplicar**.

6.7.2.2 HTTPS

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS con su PC. El HTTPS puede proteger la autenticidad de la página en todo tipo de sitios web, cuentas seguras y mantener privadas las comunicaciones, la identidad y la navegación web del usuario.

Le recomendamos habilitar el servicio HTTPS. Si este servicio está deshabilitado, puede haber riesgos de fuga de datos de comunicación.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Servicio del sistema**>**HTTPS**.

Paso 2 Hacer clic para habilitar la función HTTPS.

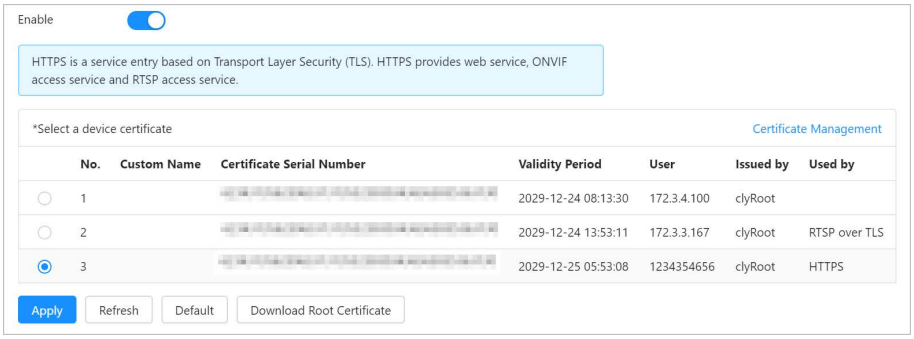
Después de habilitar HTTPS, TLSv1.1 y versiones anteriores se seleccionan de forma predeterminada. Pero hay un riesgo de seguridad para habilitar las versiones anteriores de TLSv1.1. Ser cauteloso.

Paso 3 Seleccione el certificado del dispositivo.

Si no hay ningún certificado en la lista, haga clic en**Gestión de certificados**en la barra de navegación izquierda.

Para obtener más información, consulte "6.7.4.2 Instalación del certificado de CA de confianza".

Figura 12-1 HTTPS



Etapa 4 Hacer clic**Aplicar**.

Resultado

Ingrese http://(dirección IP) en la barra de direcciones del navegador para iniciar sesión.

- Si el certificado se instaló correctamente, se mostrará la página de inicio de sesión.
- Si el certificado no se ha instalado, el sistema solicita errores de certificado.

6.7.3 Defensa de Ataque

6.7.3.1 Cortafuegos

Configure el firewall para limitar el acceso al dispositivo.

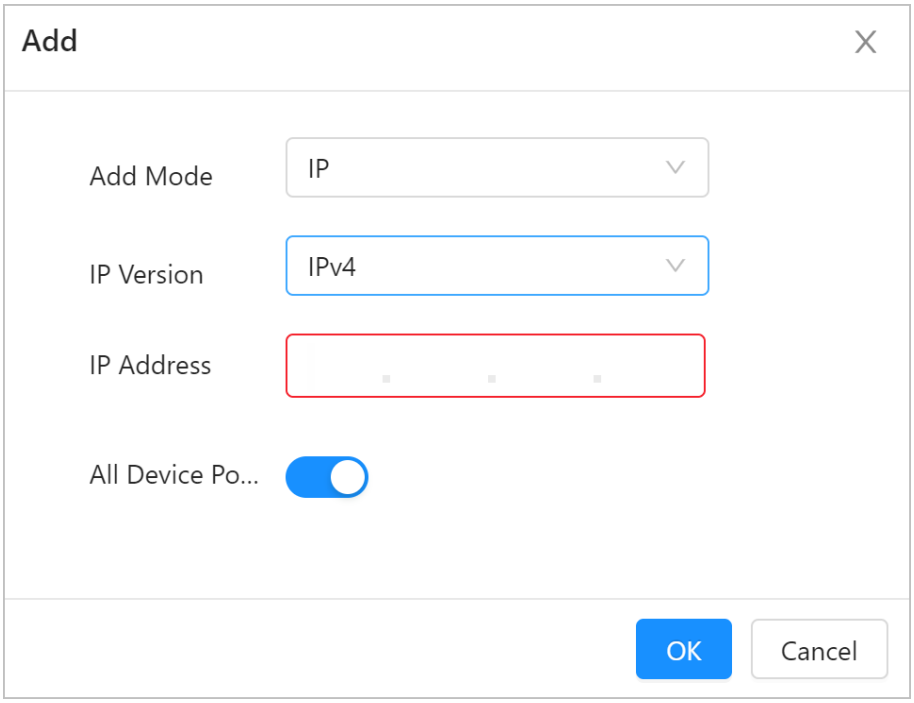
Paso 1 Seleccionar**Seguridad**>**Ataque Defensa**>**cortafuegos**. Hacer

Paso 2 clic para habilitar la función de cortafuegos.

Paso 3 Seleccione el modo:**Lista de permitidos**y**Lista de bloqueos**. Hacer

Etapa 4 clic**Agregar**.

Figura 12-1 Cortafuegos



- **Lista de permitidos**: Solo cuando la IP/MAC de su computadora está en la lista de permitidos, puede acceder al dispositivo. Los puertos son los mismos.
- **Lista de bloqueos**: Cuando la IP/MAC de su computadora está en la lista de bloqueo, no puede acceder al dispositivo. Los puertos son los mismos.

- La IP y MAC del dispositivo no se pueden configurar en la lista de permitidos o en la lista de bloqueados.
- Al agregar la dirección MAC, no puede configurar el puerto.
- La verificación de la dirección MAC solo tiene efecto cuando la dirección IP del terminal y la PC del usuario están en la misma LAN.
- Cuando se accede a la terminal a través de WAN, el sistema solo puede verificar la dirección MAC de el enrutador

Paso 5 Configure los parámetros.

Tabla 12-1 Descripciones de los parámetros del cortafuegos

Parámetro	Descripción
Agregar modo	Seleccione Dirección IP, Segmento IP, Dirección MAC o Todas las direcciones IP. ● **IP**: Seleccione la versión de IP e ingrese la dirección IP del host. ● **Segmento IP**: seleccione la versión de IP y, a continuación, introduzca la**Dirección de inicio** y**dirección final**del segmento ● **MAC**: Ingrese la dirección MAC que se agregará.
Dirección IP	Establecer como dirección IP de los dispositivos incluidos en la lista blanca o lista negra.
Puerto de inicio	Configure el puerto de acceso. Permita que los terminales en la lista de permitidos o en la lista de bloqueo accedan a su puerto designado.
Puerto final	

Paso 6 Hacer clic**DE ACUERDO**.

Paso 7 El sistema vuelve a la**cortafuegos**página. Hacer clic**Aplicar**.

6.7.3.2 Bloqueo de cuenta

Configure los tiempos permitidos de intentos de inicio de sesión y el tiempo de bloqueo para mejorar la seguridad.

Paso 1 Seleccionar**Seguridad**>**Ataque Defensa**>**Bloqueo de cuenta**. Configure el intento de

Paso 2 inicio de sesión y el tiempo de bloqueo para la cuenta del dispositivo.

- **Intento de inicio de sesión**: límite superior de intentos de inicio de sesión. Si ingresa consecutivamente una contraseña incorrecta superior al valor configurado, la cuenta se bloqueará.
- **Tiempo de bloqueo**: El período durante el cual no puede iniciar sesión después de que los intentos de inicio de sesión alcancen el límite superior.

Figura 12-1 Bloqueo de cuenta

Paso 3 Hacer clic**Aplicar**.

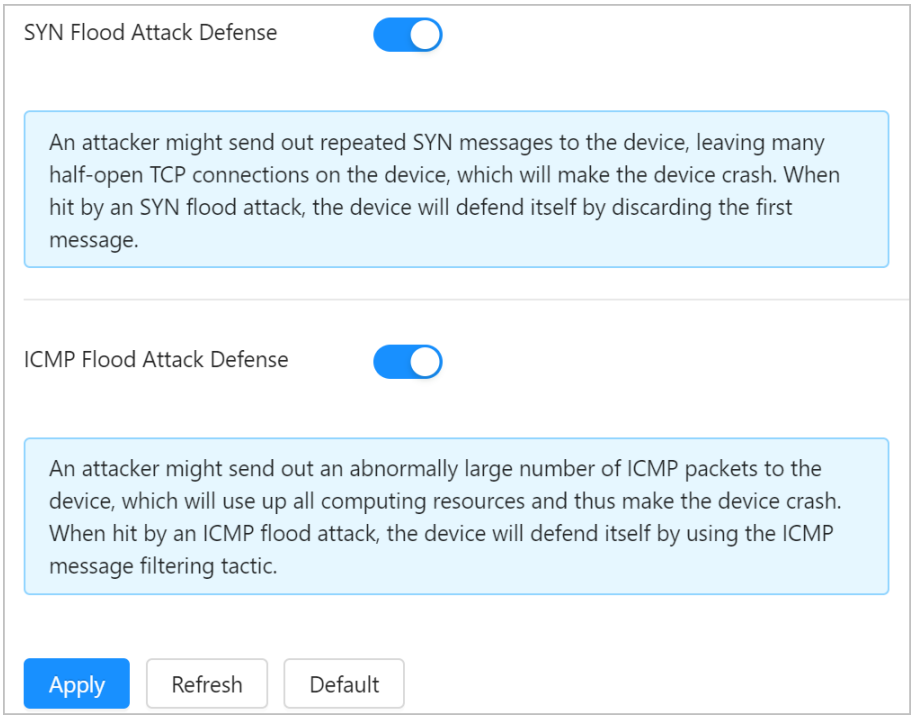
6.7.3.3 Ataque Anti-DoS

Puedes habilitar**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundación ICMP**para defender el dispositivo contra el ataque Dos.

Paso 1 Seleccionar**Seguridad**>**Ataque Defensa**>**Ataque Anti-DoS**. Hacer

Paso 2 clic junto a**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundación ICMP**a defender el dispositivo contra el ataque Dos.

Figura 12-1 Ataque Anti-DoS



Paso 3 Hacer clic**Aplicar**.

6.7.4 Certificado CA

6.7.4.1 Instalación del certificado del dispositivo

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS con su PC.

6.7.4.1.1 Creación de certificado

Crear certificado en el dispositivo.

Procedimiento

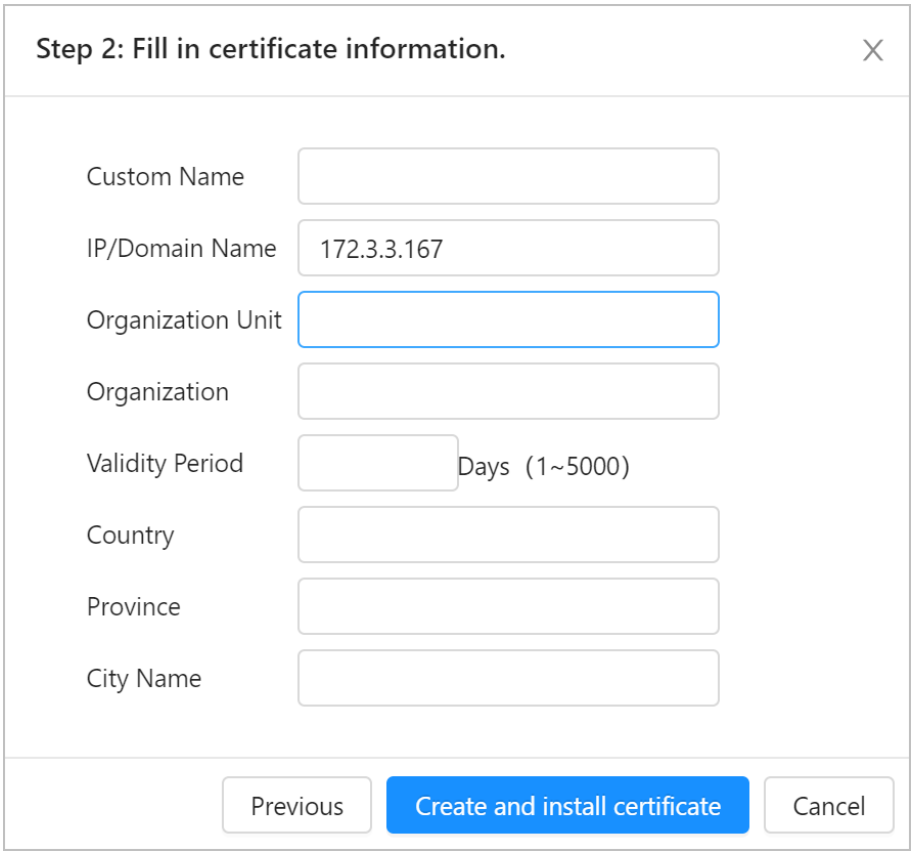
Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado de dispositivo**. Hacer clic

Paso 2 **Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Crear certificado**y luego haga clic en**Próximo**.

Etapa 4 Introduzca la información del certificado.

Figura 12-1 Información del certificado (1)



Paso 5 Hacer clic**Crear e instalar certificado**.

Una vez que el certificado se haya creado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**página.

Operaciones relacionadas

- Edición del nombre personalizado del certificado

  Hacer clic**Entrar en el modo de edición**, puede editar el nombre personalizado del certificado.
- Descargando Certificado Haga clic para descargar el certificado.
- Eliminación de certificado

  Haga clic para eliminar el certificado.

6.7.4.1.2 Solicitud e importación del certificado de CA

Importe el certificado de CA de terceros al dispositivo.

Procedimiento

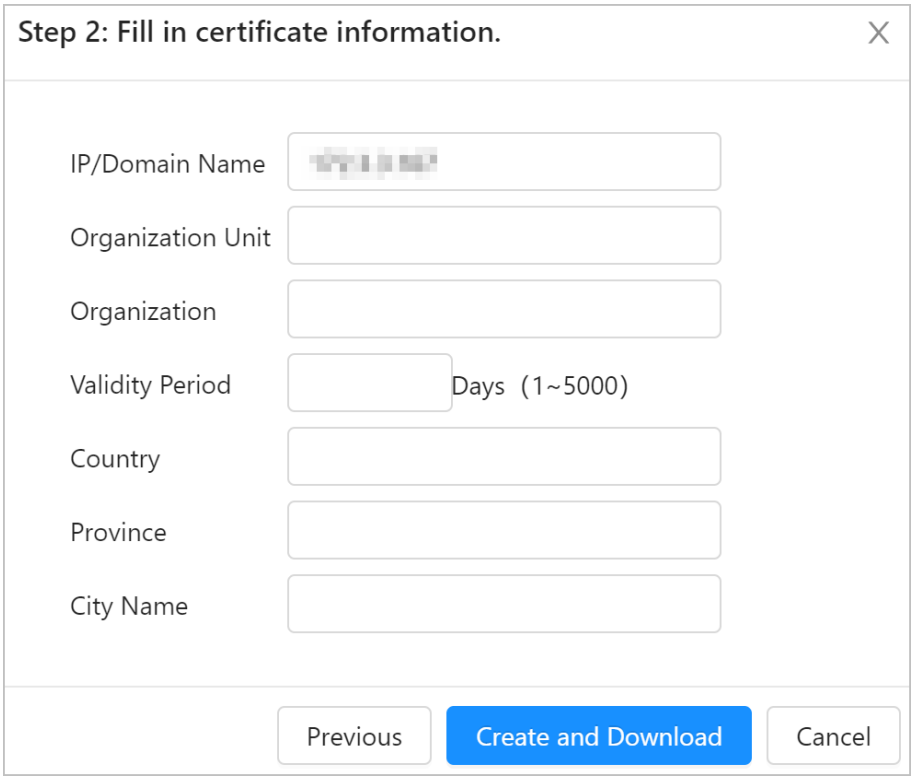
Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado de dispositivo**. Hacer clic

Paso 2 **Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Solicitar Certificado CA e Importación (Recomendado)**y luego haga clic en**Próximo**.

Etapa 4 Introduzca la información del certificado.

Figura 12-1 Información del certificado (2)



Paso 5 Hacer clic**Crear y descargar**. Guarde el archivo de solicitud en su PC.

Paso 6 Aplique el certificado de CA de la autoridad de certificación de terceros.

Paso 7 Importe el certificado de CA firmado.

1) Guarde el certificado de CA en la PC.

2) hacerPaso 1 aPaso 3 y haga clic en**Navegar**para seleccionar el certificado CE firmado.

3) Haga clic**Instalar e Importar**.

Una vez que el certificado se haya creado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**página.

- Hacer clic**Recrear**para volver a crear el archivo de solicitud.
- Hacer clic**Importar más tarde**para importar el certificado la próxima vez.

Operaciones relacionadas

- Edición del nombre personalizado del certificado

  Hacer clic**Entrar en el modo de edición**, puede editar el nombre personalizado del certificado.
- Descargando Certificado Haga clic para descargar el certificado.
- Eliminación de certificado

  Haga clic para eliminar el certificado.

6.7.4.1.3 Instalación de un certificado existente

Importe el certificado de terceros existente a la cámara. Cuando solicite el certificado de terceros, también debe solicitar el archivo de clave privada y la contraseña de clave privada.

Procedimiento

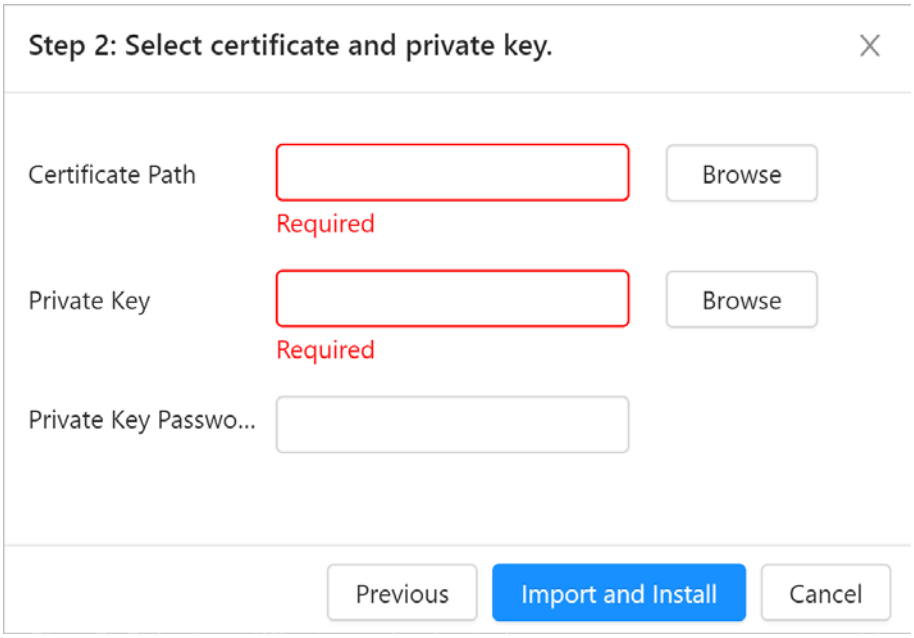
Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado de dispositivo**. Hacer clic

Paso 2 **Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Instalar certificado existente**y haga clic en**Próximo**.

Etapa 4 Hacer clic**Navegar**para seleccionar el certificado y el archivo de clave privada, e ingrese la contraseña de la clave privada.

Figura 12-1 Certificado y clave privada



Paso 5 Hacer clic**Importar e instalar**.

Una vez que el certificado se haya creado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**página.

Operaciones relacionadas

- Edición del nombre personalizado del certificado

  Hacer clic**Entrar en el modo de edición**, puede editar el nombre personalizado del certificado.
- Descargando Certificado Haga clic para descargar el certificado.
- Eliminación de certificado

  Haga clic para eliminar el certificado.

6.7.4.2 Instalación del certificado de CA de confianza

El certificado CA es un certificado digital para la identidad legal del dispositivo. Por ejemplo, cuando el dispositivo accede a la LAN a través de 802.1x, se requiere el certificado de CA.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificados de CA de confianza**.

Paso 2 Seleccionar**Instalación de certificado de confianza**. Hacer clic**Navegar**para

Paso 3 seleccionar el certificado.

Una vez que el certificado se haya creado correctamente, puede ver el certificado creado en la **Certificado de CA de confianza**página.

Operaciones relacionadas

- Edición del nombre personalizado del certificado

  Hacer clic**Entrar en el modo de edición**, puede editar el nombre personalizado del certificado.

- Descargando Certificado Haga clic para descargar el certificado.

- Eliminación de certificado

  Haga clic para eliminar el certificado.

6.7.5 Cifrado de vídeo

El dispositivo admite el cifrado de audio y video durante la transmisión de datos.

Le recomendamos que habilite la función de cifrado de video. Puede haber riesgo de seguridad si esta función es desactivado.

Paso 1 Seleccionar**Seguridad**>**Cifrado de vídeo**.

Paso 2 Configure los parámetros.

Figura 12-1 Cifrado de video

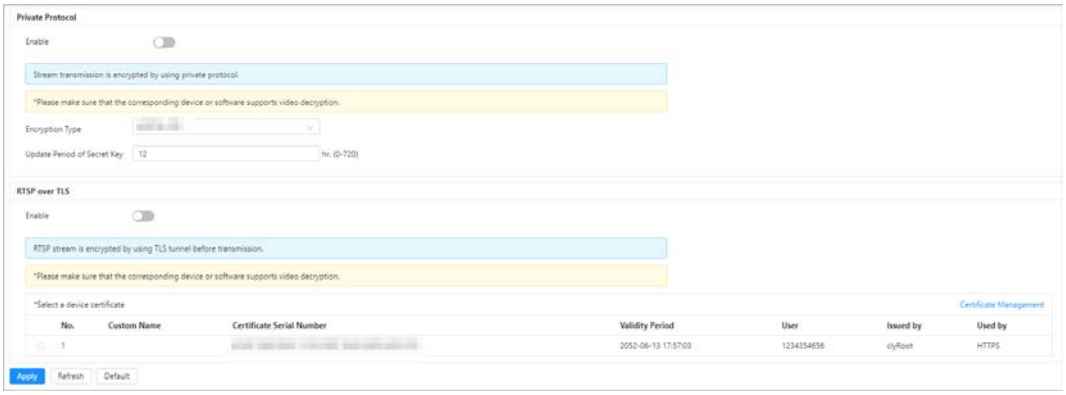


Tabla 12-1 Descripciones de los parámetros de encriptación de video

Área	Parámetro	Descripción
Protocolo privado	Permitir	Habilita el cifrado de tramas de transmisión mediante el uso de un protocolo privado. Puede haber un riesgo de seguridad si este servicio está deshabilitado.
	Tipo de cifrado	Utilice la configuración predeterminada.
	Período de actualización de Llave secreta	Período de actualización de la clave secreta. Rango de valores: 0–720 horas. 0 significa nunca actualizar la clave secreta. Valor predeterminado: 12.
RTSP sobre TLS	Permitir	Habilita el cifrado de transmisión RTSP mediante TLS. Puede haber un riesgo de seguridad si este servicio está deshabilitado.

Área	Parámetro	Descripción
	Seleccione un dispositivo certificado	Seleccione un certificado de dispositivo para RTSP sobre TLS.

Paso 3 Hacer clic**Aplicar**.

6.8 Registro

Ver y descargar los videos dentro de los períodos especificados.

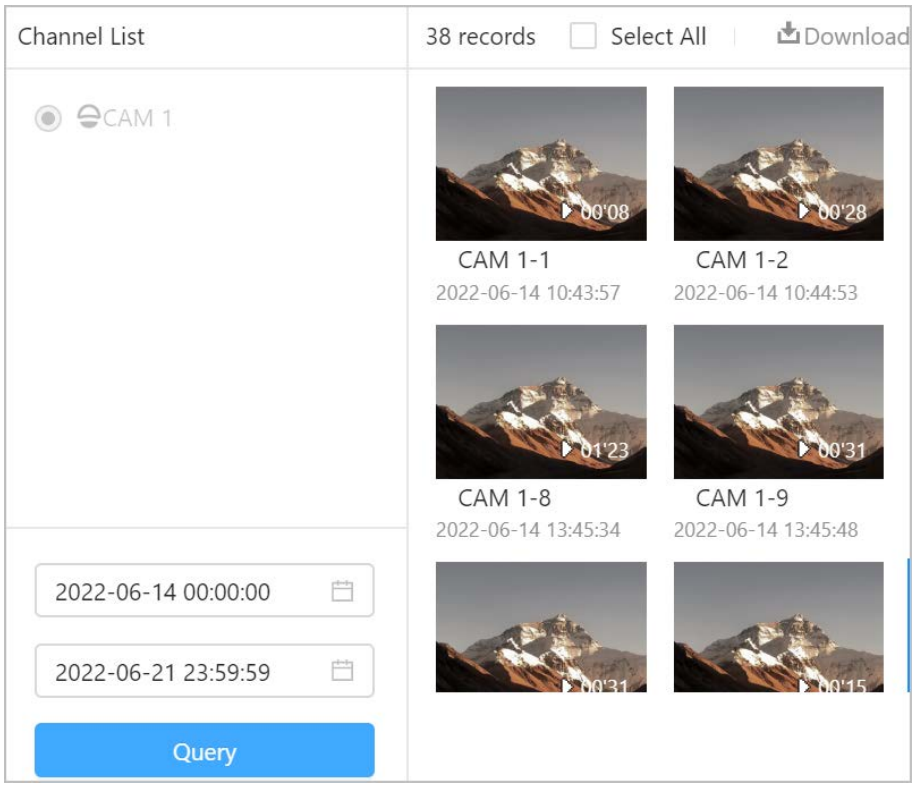
El dispositivo solo tiene un canal.

Paso 1 Inicie sesión en la página web, haga clic en**Registro**.

Paso 2 Establezca la hora de inicio y finalización y, a continuación, haga clic en**Buscar**para ver los videos de grabación.

Seleccione uno o varios videos de grabación y luego haga clic en para descargarlos.

Figura 6-44 Ver videos de grabación



6.9 Imagen

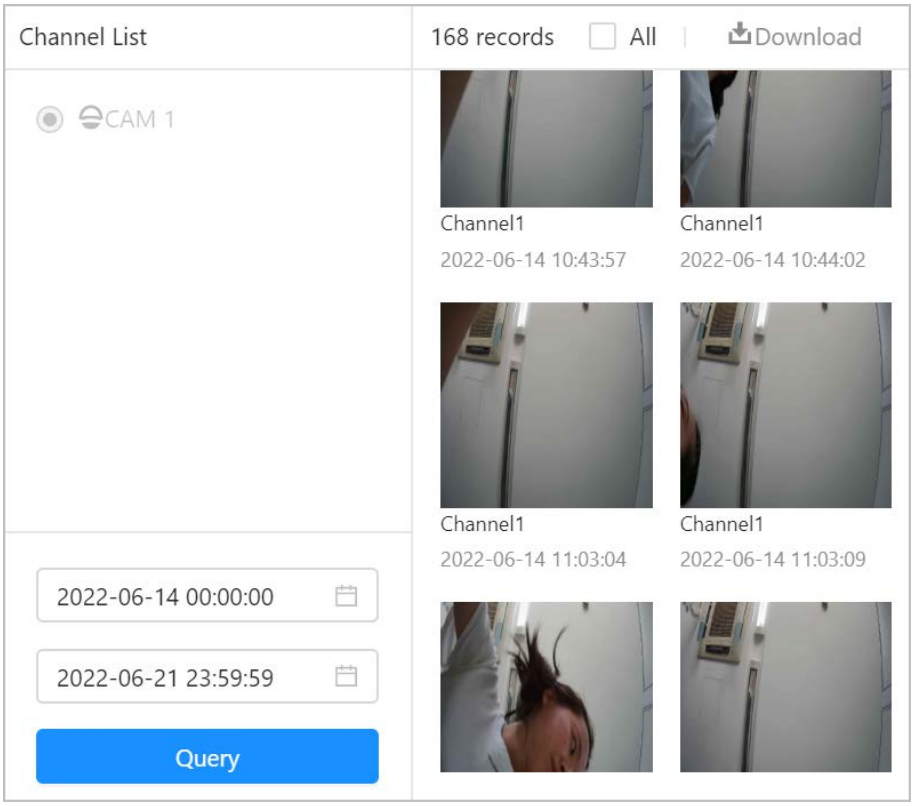
Ver y descargar las imágenes dentro de los períodos especificados.

El dispositivo solo tiene un canal.

Paso 1 Inicie sesión en la página web, haga clic en**Imagen**.

Paso 2 Establezca la hora de inicio y finalización y, a continuación, haga clic en**Buscar**para ver las fotos. Seleccione una o varias imágenes y luego haga clic para descargarlas.

Figura 6-45 Ver imágenes



Apéndice 1 Recomendaciones sobre ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso.
- No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

2.**Actualice el firmware y el software del cliente a tiempo**

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo:

1.Protección Física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en un gabinete y una sala de computadoras especiales, e implemente un control de permisos de acceso y administración de claves bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2.**Cambie las contraseñas regularmente**

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3.**Establecer y actualizar contraseñas Restablecer información a tiempo**

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4.**Habilitar bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión varias veces con la contraseña incorrecta, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre

1024–65535, lo que reduce el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

6.**Habilitar HTTPS**

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

7.**Enlace de dirección MAC**

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de identidad ARP.

8.**Asigne cuentas y privilegios de manera razonable**

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

9.**Deshabilite los servicios innecesarios y elija modos seguros**

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

10**Transmisión encriptada de audio y video**

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión encriptada para reducir el riesgo de robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11**Auditoría segura**

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12**Registro de red**

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13**Construir un entorno de red seguro**

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder a la

dispositivo.

Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para conocer los anuncios de seguridad y las recomendaciones de seguridad más recientes.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883